出國報告（出國類別：開會）

出席 Black Hat Asia 2023
出國報告書

服務機關：數位發展部資通安全署

姓名職稱：邱俊惟高級分析師

張祚嘉高級資安程式設計師

派赴國家：新加坡

出國期間：112 年 5 月 8 日至 13 日

報告日期：112 年 8 月 1 日

摘 要

Black Hat （黑帽）是國際知名的資訊安全系列活動，是世界著名的資安活動之一，在 112 年間包含本次參與的亞洲會議，還有美國、歐洲、中東和非洲等共四次會議，為資訊安全領域提供最新的研究、發展和趨勢資訊。

在黑帽系列活動中，本次參加於 112 年 5 月 9 日至 12 日位在新加坡的亞洲會議，期間包含 2 天工作坊及 2 天研討會，其工作坊課程及各場次演講是根據全球資安社群的需求而設計的，讓參與者瞭解並掌握最新的網路攻擊手法與趨勢，建構一個國際駭客社群交流的平台，強化對未來資訊安全防護的思考，進一步推動全球資訊安全領域的發展。

內容

壹、目的

Black Hat （黑帽）是國際知名的資訊安全系列活動，此活動原是由一年一度會議行程發展而來，現已成為世界著名的資安活動之一，並為資訊安全領域提供最新的研究、發展和趨勢資訊。

在黑帽系列活動中，簡報和培訓是根據全球資安社群的需求而設計的。這些活動旨在聚集業界內最優秀的專業人才，提供最新的漏洞資訊和研究，並促進各個職業級別專業人士之間的成長和合作。黑帽每年在美國、歐洲和亞洲等各地舉辦簡報和培訓活動，成為精英安全研究人員和培訓師尋找受眾的首選場所，參與黑帽活動可以讓參與者瞭解並掌握最近期的攻擊手段，並強化對未來資訊安全防禦對策的思考，建構一個國際駭客社群交流的平台，進一步推動全球資訊安全領域的發展。

貳、過程

本次參加的 Black Hat ASIA 為期四天，自 112 年 5 月 9 日至 5 月 12 日止，參加場次如下：

日期	活動主題
5 月 9 日	A Complete Practical Approach to Malware Analysis and Memory Forensics - 2023 Edition （從實際操作角度看惡意程式分析和記憶體取證 - 2023 年版）
5 月 10 日	A Complete Practical Approach to Malware Analysis and Memory Forensics - 2023 Edition （從實際操作角度看惡意程式分析和記憶體取證 - 2023 年版）

5 月 11 日	When Knowledge Graph Meets TTPs: Highly Automated and Adaptive Executable TTP Intelligence for Security Evaluation （當知識圖譜遇上 TTPs：高度自動化和適應性執行 TTP 智能安全評估）
	Operation Clairvoyance: How APT Groups Spy on the Media Industry （千里眼行動：APT 組織如何監視媒體行業）
	Dirty Stream Attack, Turning Android Share Targets Into Attack Vectors （惡意串流攻擊：將 Android 共享目標轉化為攻擊向量）
	Insider Threats Packing Their Bags With Corporate Data （將企業數據打包的內部威脅）
	Leveraging Streaming-Based Outlier Detection and SliceLine to Stop Heavily Distributed Bot Attacks （利用基於串流的異常檢測和 SliceLine 來阻止大規模分佈式機器人攻擊）
5 月 12 日	Sweet Dreams: Abusing Sleep Mode to Break Wi-Fi Encryption and Disrupt WPA2/3 Networks （甜美夢境：濫用睡眠模式破解 Wi-Fi 加密並干擾 WPA2/3 網路）
	Security Advocacy Shouldn't Be for Security Professionals: An Analysis of How the Industry Misses the Mark and How We Can Improve （安全倡議不應僅針對安全專業人士：分析行業的不足之處以及我們如何改進）

	A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks （每天慢跑無法阻止駭客：對健身追踪社交網路中終端隱私區域的推論攻擊）
	Phoenix Domain Attack: Vulnerable Links in Domain Name Delegation and Revocation （鳳凰網域攻擊：網域委派和撤銷中的弱點連結）
	Cloudy With a Chance of Exploits: Compromising Critical Infrastructure Through IIoT Cloud Solutions （雲端服務中的風險：透過工業物聯網雲端解決方案所危及的關鍵基礎設施）

參、會議紀要

一、A Complete Practical Approach to Malware Analysis and Memory Forensics - 2023 Edition（從實際操作角度看惡意程式分析和記憶體取證 - 2023 年版，講者：Monnappa K A）

此實作研習是從實際操作角度看惡意程式分析和記憶體取證，以先建立相關先備知識再透過操作虛擬機器（Virtual Machine，VM）來分析各種惡意程式的練習，以期望所有參與課程之學員皆能對數位鑑識有基本的理解與能力。

研習課程為期兩天，第一天先進行惡意程式的概念及基礎分析解說，惡意程式分析包含靜態、動態及記憶體分析（圖 1），第二天則進一步從記憶體分析惡意程式，並透過程序及網路活動進行檢視分析。

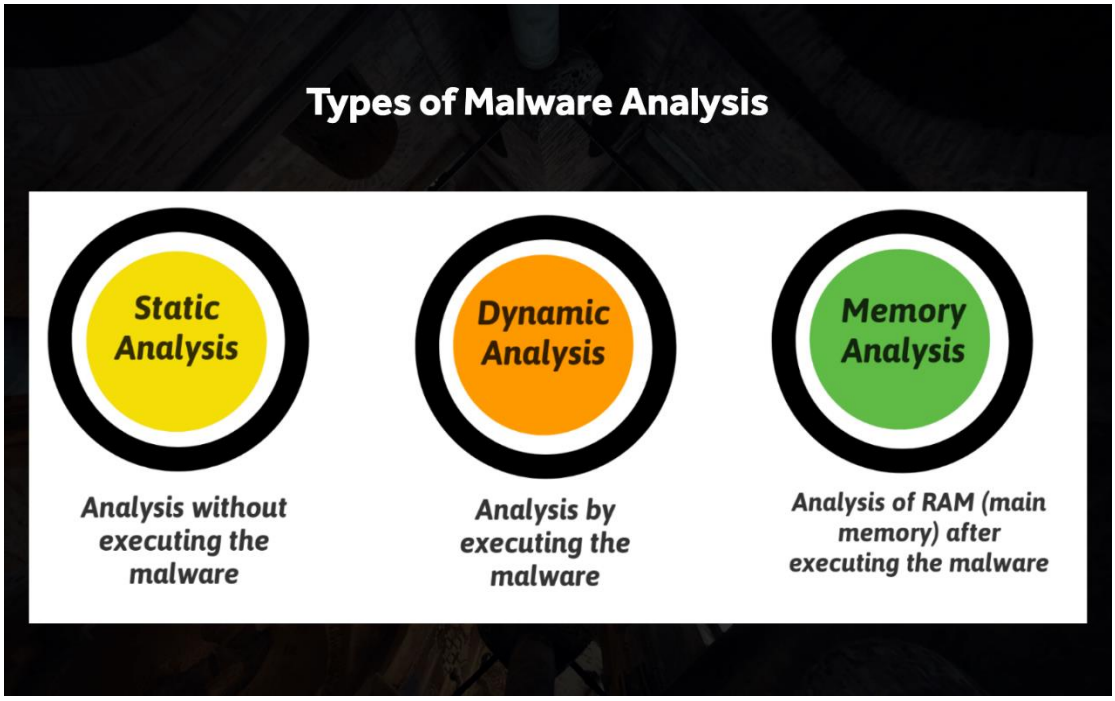


圖 1：惡意程式分析類型（資料來源：講者簡報）

在此研習提到以下三種惡意程式分析的方法：

(一) 靜態分析（Static Analysis）：靜態分析是透過檢查惡意程式的檔案或程式碼本身，而不執行它們來進行分析。這包括檢查檔案的結構、程式碼特徵、內部字串、函式呼叫等。靜態分析可使用反組譯器、靜態程式碼分析工具和字串提取工具等來分析惡意程式。

(二) 動態分析（Dynamic Analysis）：動態分析是在受控環境如虛擬機器中執行惡意程式，觀察其行為和互動。這包括監測軟體的系統呼叫、檔案系統操作、網路通訊和註冊表修改等，動態分析可使用虛擬機器或沙盒等虛擬環境，再搭配使用監控工具來捕捉和分析惡意程式的活動。

(三) 記憶體分析（Memory Analysis）：記憶體分析是在檢查和分析惡意程式於電腦記憶體中的活動和資料，透過分析記憶體內容，可獲取有關惡

意程式執行過程、通訊活動、加密金鑰、注入技術和已載入模組等重要資訊。

工欲善其事，必先利其器，在課程開始前，首先需要準備虛擬環境和工具軟體，為避免影響個人電腦或是網路，一律都是在電腦上架設虛擬機器且封鎖網路後才進行，以免在執行惡意程式分析時，造成不必要的損害。虛擬機器一般常見的有 VMware、VirtualBox 和 Hyper-V 等軟體，其可在單一的實體電腦上執行多個虛擬作業系統，意即可以在同一台電腦上同時執行不同的作業系統，例如 Windows、Linux 或 macOS，而無需進行實體硬體的分割或重啟即可模擬完整的電腦環境，虛擬環境可選擇其虛擬的硬體，包括處理器（CPU）、記憶體（RAM）、硬碟和其他周邊設備，其快照功能可重複重現所需的前次環境狀態，亦可從其它電腦複製映像檔再用虛擬機器載入來再現複製時的狀態。虛擬環境準備足夠後，以下解說課程中介紹應用的檢測軟體：

(一) Volatility：Volatility 記憶體分析框架是套開源軟體，用於數位取證和惡意程式分析，可從電腦記憶體中提取數據，以了解系統運作時的狀態、行為和事件，通過分析記憶體快照，Volatility 可以找到攻擊活動、惡意行為、系統漏洞和其他重要資訊的蛛絲馬跡，進一步幫助調查人員追蹤和分析數位犯罪行為。

(二) Comae Memory Toolkit：Comae Memory Toolkit 是為記憶體收集和轉換用的工具組，其中 DumpIt 程式可自記憶體快照，支援 32 位元和 64 位元電腦，並可在 Windows 上進行快照，以了解系統運作時的狀態和事件，可增強數位取證和惡意程式分析的能力。

(三) Exeinfo PE：Exeinfo PE 是檔案檢視工具，常用於查看和分析 PE（Portable Executable）檔案的資訊，其可提供關於 EXE 和 DLL 檔案的詳細資訊，例如程式設計編譯器資訊、加殼狀態（加密保護方式）、進

入點位址、輸出表和輸入表等，這些資訊對於程式分析、破解和逆向工程，具一定程度的幫助效果。

(四) Explorer Suite ：Explorer Suite 是一整套包含 CFF Explorer、Quick Unpack、Resource Hacker 和 PE Detective 等工具軟體包，其可對檔案頭、區段表、導入表、導出表、資源表進行編輯和檢視，並提供進階功能，如資源編輯、節區屬性修改和脫殼操作等，使用戶可以對 PE 檔案進行更深入的分析和修改，於逆向工程中此工具包極具實用。

(五) IDA：IDA 是套二進制程式碼分析工具，其可將執行的二進制指令轉換成組合語言，幫助分析師深入理解程式的運作方式，從機器執行的程式碼中生成易於閱讀的組合語言程式碼，使複雜的程式碼更容易理解和分析。

(六) Noriben：Noriben 是一款動態分析惡意程式的開源工具，能夠捕捉並記錄惡意樣本的活動，包括檔案創建、程序生成、系統註冊表修改和網路連接等，並提供詳細結果。

(七) PeStudio：PeStudio 是用於分析 Windows 可執行檔案（EXE、DLL、SYS 等）的工具，其可進行深入的靜態分析，檢查檔案的多個層面，包括文件屬性、區段、函數的輸入和輸出、檔案簽名、資源、相依性等，並能檢測潛在的安全風險和可疑行為，例如檔案的加密、壓縮和去模糊處理等，是一套功能豐富的工具。

(八) Process Hacker ：Process Hacker 是開源的程式管理和系統監控工具，用於 Windows 系統，可提供豐富的功能和詳細的系統資訊，讓用戶能夠監控和管理正在運作的程式、服務、網路連接和系統性能等，常用於系統管理、程式分析、軟體開發和惡意程式分析。

(九) Python：Python 可在多種作業系統上執行，包括 Windows、macOS 和 Linux ，是種具高度可移植性的語言，其在各個領域都有廣泛的應用，

包括網站開發、資料分析、機器學習、人工智慧、科學計算、自動化測試和網絡爬蟲等，部份數位鑑識所需的程式碼亦使用此語言開發。

(十) Resource Hacker：Resource Hacker 是套資源編譯器，可供編輯.rc 檔案中的資源，亦也有反編譯器的功能，可查看副檔名為.exe、.dll 和.scr 等檔案，讓使用者能根據需求進行資源的編輯和修改，以達到修改特定資源的目的。

(十一) Sysinternals Suite：Sysinternals Suite 是由 Microsoft 公司開發的一組工具集，專為 Windows 系統的故障排除和系統管理而設計，套件中包含了多個工具，涵蓋了各種系統管理和故障排除的方面，可用於監控系統性能、分析和除錯應用程序、檢測和移除惡意程式、管理系統程序和服務、監測網路連接等，有助於 Windows 系統的管理。

(十二) x64dbg：x64dbg 是於 64 位元 Windows 所使用的反編譯和除錯工具，具有支援多種除錯功能，例如斷點、步進、追踪等，讓用戶能夠觀察和控制應用程序的執行流程，是反編譯和除錯任務的常用工具之一。

在做完所有預備工作後，即展開惡意程式分析，依序說明如下：

(一) 惡意程式靜態分析可分以下步驟：

1. 確定檔案類型：確定檔案類型可有助於分析惡意程式的目標架構，如檔案類型是 PE，則可推斷目標是 Windows 系統，但副檔名並非檔案類型的絕對指標，可利用 PeStudio（Windows）或 File utility（Linux）工具進行檔案類型確認（圖 2），可發現部份惡意程式是會偽造其為可執行檔的身份。

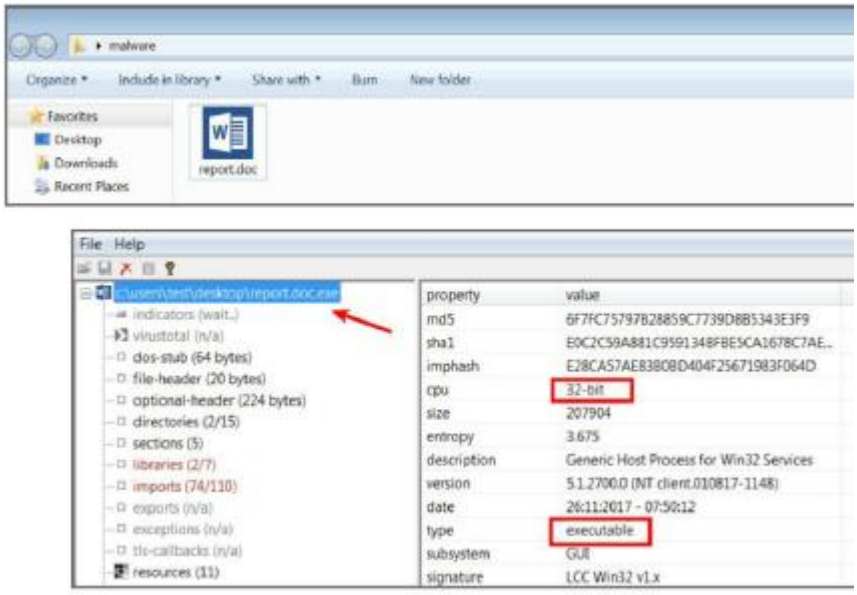


圖 2：EXE 可執行檔偽裝成 Word 檔（資料來源：講者簡報）

2. 加密雜湊（Cryptographic Hash）：將惡意程式利用 md5sum、sha256sum、shalsum（Linux）或 PeStudio（Windows）等工具去運算出 md5、sha1 或 sha256 的唯一辨識值（圖 3），並可於線上（例如：VirusTotal）確認該軟體是否已被識別判定。

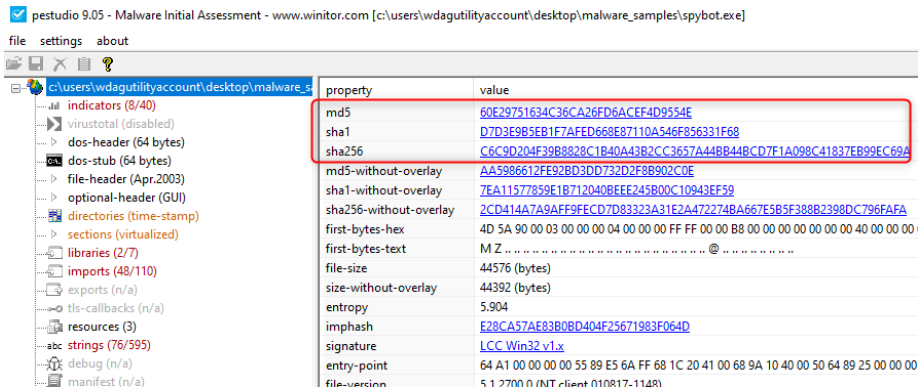


圖 3：檔案其 md5、sha1 和 sha256 的值（資料來源：自測試環境截圖）

3. 字串（Strings）：字串是存在於檔案中以 ACSII 或 UNICODE 所顯示之文字，可利用 PeStudio 或 Strings 工具提取出字串，並用於辨識惡意

程式中的功能或相關指令線索，亦可發現其包含之特定的網域名稱和檔案名稱（圖 4）。

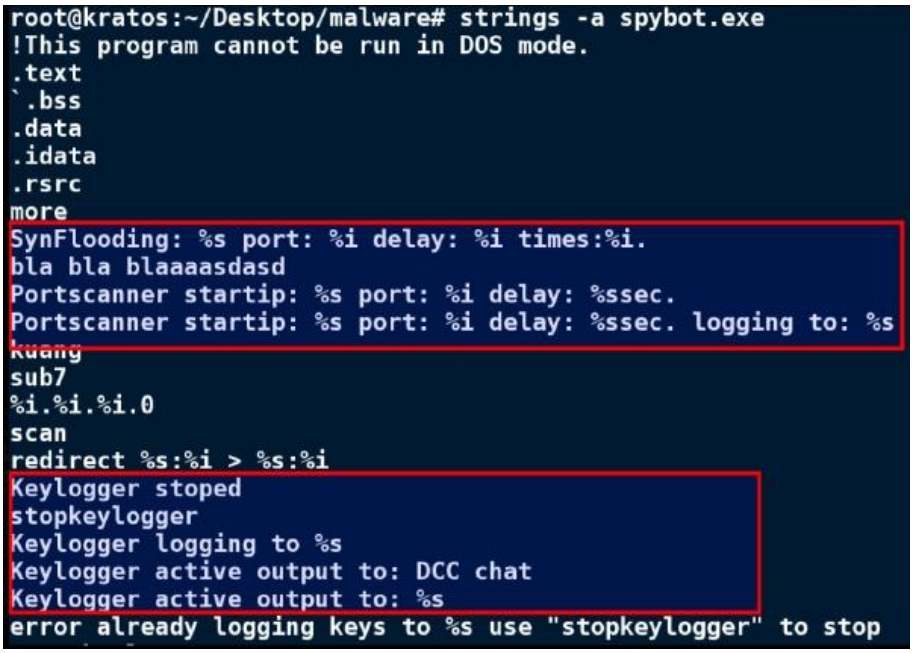


圖 4：發現檔案中包含 portscan 和 keylogger 功能（資料來源：講者簡報）

4. 檔案混淆（File Obfuscation）：惡意程式製作者常利用 UPX 加殼（packer）或加密來混淆視聽，並使其字串和函數數量變少而難以被分析，可利 Exeinfo PE 確認檔案是否經加殼（圖 5）。

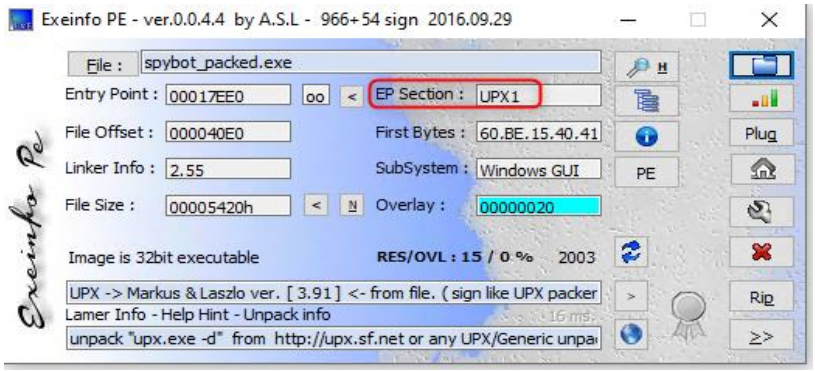


圖 5：發現檔案經 UPX 加殼（資料來源：自測試環境截圖）

5. 利用 YARA 規則：透過建立 YARA 規則來幫助分辨惡意程式樣本，其方式是建立包含字串和布林算式的規則，並將已知惡意程式其所包含的文字或是二進制模式建立 YARA 規則中，以快速辨識惡意程式（圖 6）。

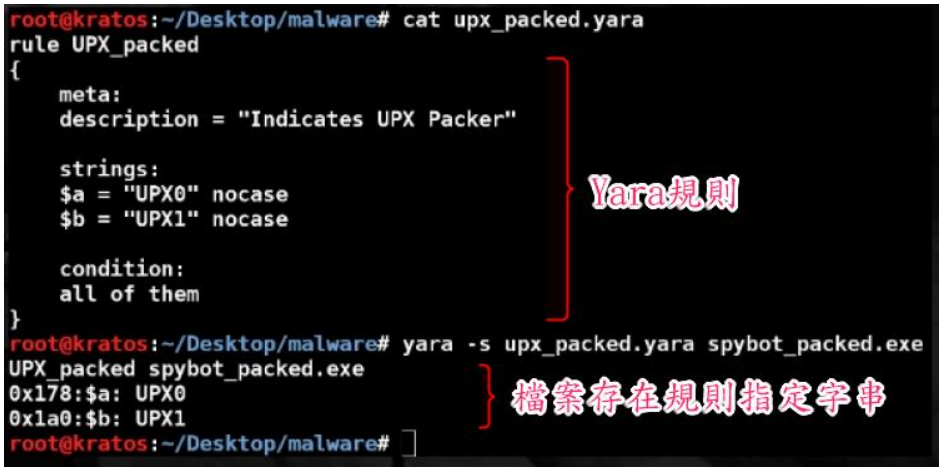


圖 6：利用 YARA 來識別惡意程式（資料來源：講者簡報加上個人註解）

6. 模糊雜湊和比對（Fuzzy Hashing & Comparison）：模糊雜湊和比對是利用比較不同檔案其相似度百分比的技術，可用於辨識相似的惡意程式版本或是變種版本，一般情況可使用 ssdeep 工具，並利用模糊雜湊比對功能，運算出樣本的相似度（圖 7）。

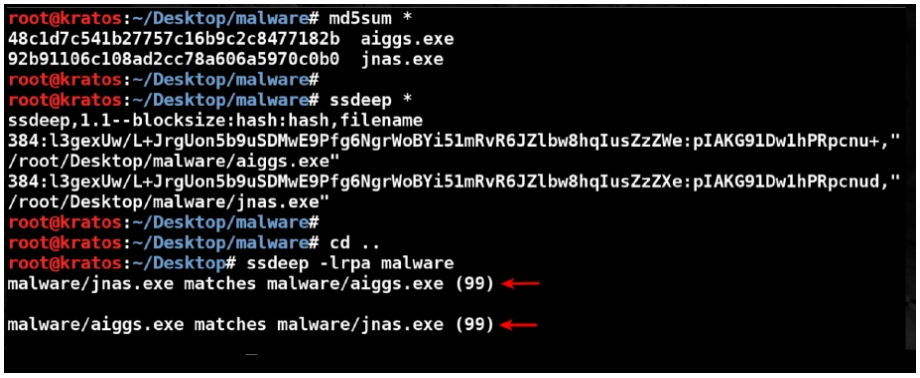


圖 7：檢測出兩個檔案的相似度高達 99%（資料來源：講者簡報）

7. 檢測 PE 的匯入項目（Inspecting PE Imports）：利用 PeStudio 工具程式檢視目標檔案是否載入多種函式庫或呼叫 API 函數，確認其函式庫及 API 的調用列表即可了解惡意程式的功能，例如可解析網域或建立 Http 連接等（圖 8）。

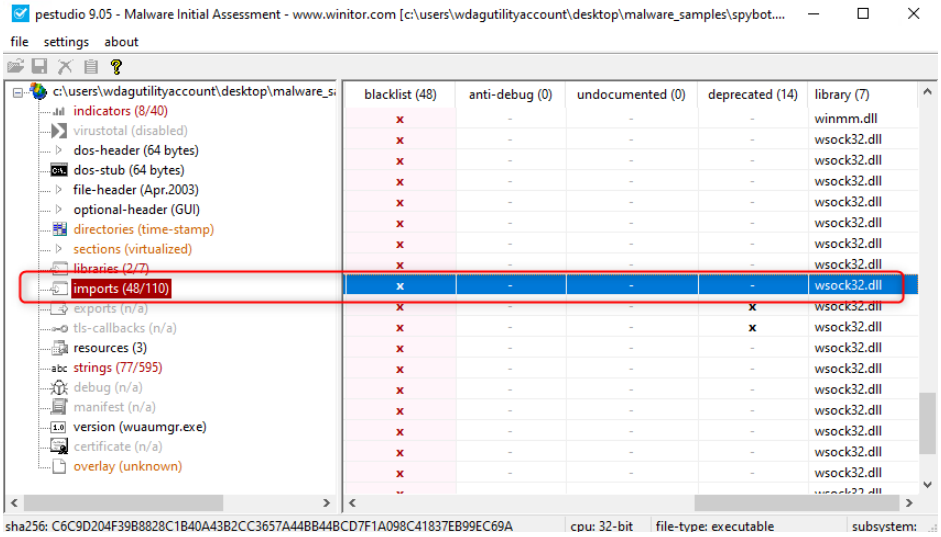


圖 8：該軟體匯入了具有網路功能的 wsock32.dll，表示其具有連網能力（資料來源：自測試環境截圖）

8. 檢測 PE 的表頭（Inspecting PE Header）：於 PeStudio 中檢視 Header（表頭）發現一些可用於分析的有用資訊，例如檔案編譯時間、匯入或匯出用函數等，將有助辨識軟體的一些異常行為（圖 9）。

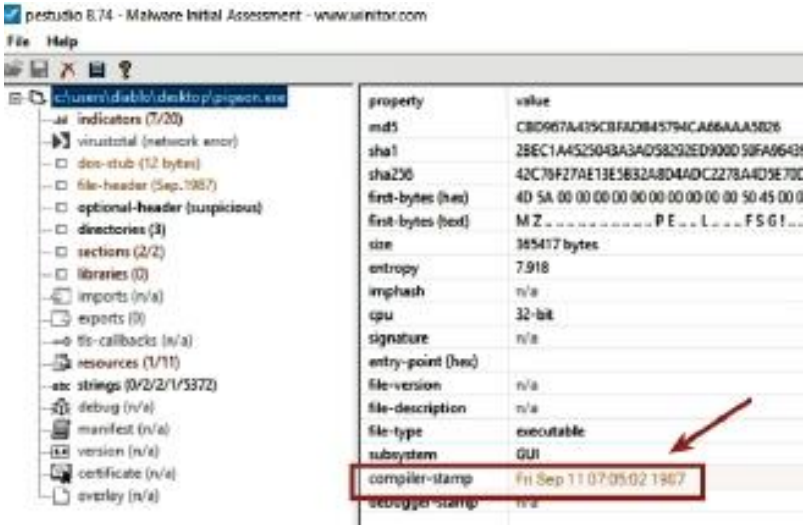


圖 9：該軟體修改編譯日期，顯示編譯時間戳印為 1987 年（資料來源：講者簡報）

程式碼分析中靜態分析具動態分析所做不到的部份，在靜態分析中常用的逆向工程軟體有 IDA、x64dbg、Ollydbg、Immunity Debugger 及 Windbg，課程使用的 IDA 是套專業反編譯軟體，當程式碼執行時，利用設定斷點來暫停執行程式碼，並可將原始機器碼轉換成組合語言或高階語言，可有助於理解程式及其邏輯，在分析前，應先理解何為呼叫 API（call Application Programming Interface ），其作用是在調用函式，不同的函式可執行預先設定好的操作，其將參數推送到堆疊中，然後函式將返回值存儲在 EAX/RAX 暫存器中，其實我們只要檢查函式就能確定其功能，查看呼叫 API 即可明白惡意程式與環境互動的可能狀況，我們可以在 MSDN 網站上搜尋到一些呼叫 API 的相關資料，例如 CreateFileA function 和 InternetConnectA function（圖 10）。

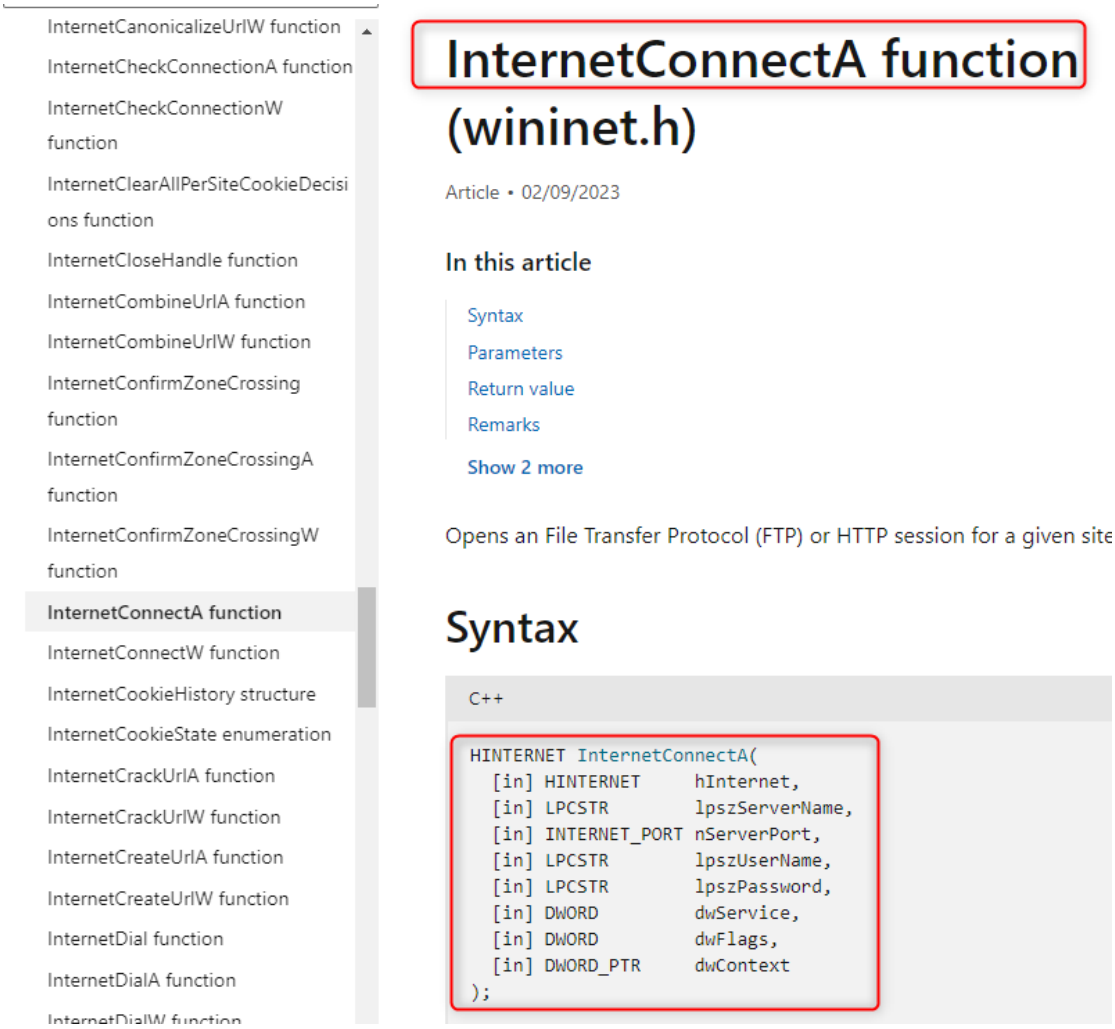


圖 10：InternetConnectA function 具網路傳輸之功能（資料來源：MSDN 網站）

各類型的惡意程式及其可能包含的 API 介紹如下：

1. 下載器（Downloader）：是一種能夠下載其他程式的惡意程式。它通常會被用來繞過安全防護措施，先在受害者的電腦上執行，然後從遠端伺服器下載其他惡意程式並進行感染，使用 URLDownloadToFile()函式，可下載檔案並存入硬碟中，當它被調用時，通常會再搭配 ShellExecute() 或 WinExec() 來執行下載的檔案。

2. 傳送器（Dropper）：主要功能是在受害者的電腦下載其他惡意程式通常被設計成看似無害或偽裝成合法檔案，一旦執行，它會解壓縮或下載其他惡意元件到系統中，其與 Downloader 差別在於 Downloader 是下載至外部執行，Dropper 則是下載至程式內部嵌合使用，其會使用的 API 有 FindResource()、LoadResource()、SizeOfResource()及 LockResource()。
3. 鍵盤記錄器（Keylogger）：此種惡意程式用於記錄受害者在電腦上所有鍵盤或滑鼠輸入，它可以記錄使用者輸入的帳號、密碼、信用卡資訊等敏感資訊，然後將這些資訊偷偷發送到攻擊者的伺服器，其主要透過 SetWindowsHookEx() 或 GetAsyncKeyState() 來抓取鍵盤或是滑鼠事件。
4. 注入程式碼惡意程式（Code Injection Malware）：此惡意程式利用特定的技術在其他應用程式的執行時期間，將惡意程式碼注入到它們的記憶體空間中，以修改其行為或進行攻擊，其所調用的 API 有 OpenProcess()用於打開遠端程式控制、VirtualAllocEx()用於分配記憶體、WriteProcessMemory()將程式碼寫入遠端記憶體及 CreateRemoteThread()用於執行注入的惡意程式碼。
5. Http 後門（HTTP Backdoor）：用於在受感染的系統上建立一個秘密的後門通道，以便攻擊者可透過網路以 HTTP 協議來遠端控制受感染的系統，此方式可能可以繞過防火牆規則，並易與正常用戶流量結合，增加檢測難度，其所用的 API 有 InternetOpen() 或 InternetConnect() 建立 HTTP 連線、HttpOpenRequest()、HttpAddRequestHeader() 來建立 HTTP 請求、使用 HttpSendRequest() 發送 HTTP 請求以及 InternetReadFile() 來讀取回應。

接著使用 IDA 進行惡意程式解析，首先課程中檢測一個檔案名為 adobe.exe 的程式，在開啟 IDA 並載入該程式後，進入 import 頁面尋找前面介紹過惡意程式可能會使用的 API，在這裡我們發現它載入了 GetAsyncKeyState 和 GetKeyState，接著使用 xref 功能追蹤呼叫 API 的位置，在 GetAsyncKeyState 的位置觀察它的程式運作，即發現它除了會記住鍵盤輸入外，還有在進行 CreateFile 和 WriteFile 動作，因此推測這是一個會記錄按鍵輸入的鍵盤記錄器惡意程式，在設定 CreateFile 和 WriteFile 這幾個 API 的斷點（Breakpoint）後，我們使用 Debug 模式進行測試，逐步追蹤程式的執行，透過 Stack view 中找到.data.FileName 的位置，我們右鍵檢視 hex dump，即成功發現了惡意程式所記錄按鍵的存檔位置（圖 11），該檔案名為 ntuser.inf，其被加了系統隱藏屬性，必須於資料夾設定中開啟「顯示隱藏的檔案、資料夾或磁碟機」功能，才能順利於該檔案位置看到檔案。

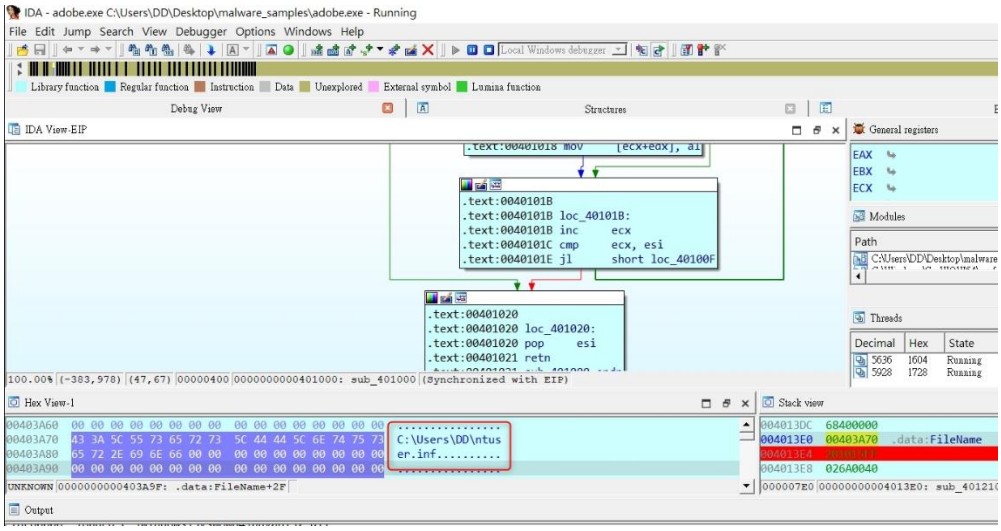


圖 11：於 IDA 中發現其存放紀錄於 C:\Users\DD\，並將檔名偽裝成 ntuser.inf（資料來源：自測試環境截圖）

Ollydbg 是款 32 位元 debug（除錯）工具，常被用來分析、反編譯和偵錯，課程中講師發了一個 LAB 模擬實驗，以名為 blob 的惡意程式案例請學員嘗試分析並解答以下問題：

1. 這個惡意程式是否有呼叫下載用的 API？

   答：經 OllyDbg 查看 API 呼叫，首先以系統管理員身份執行 OllyDbg 並載入 blob.exe，並查找其匯入的功能，即發現 API 呼叫 URLDownloadToFile()，此功能可用於下載檔案（圖 12）。

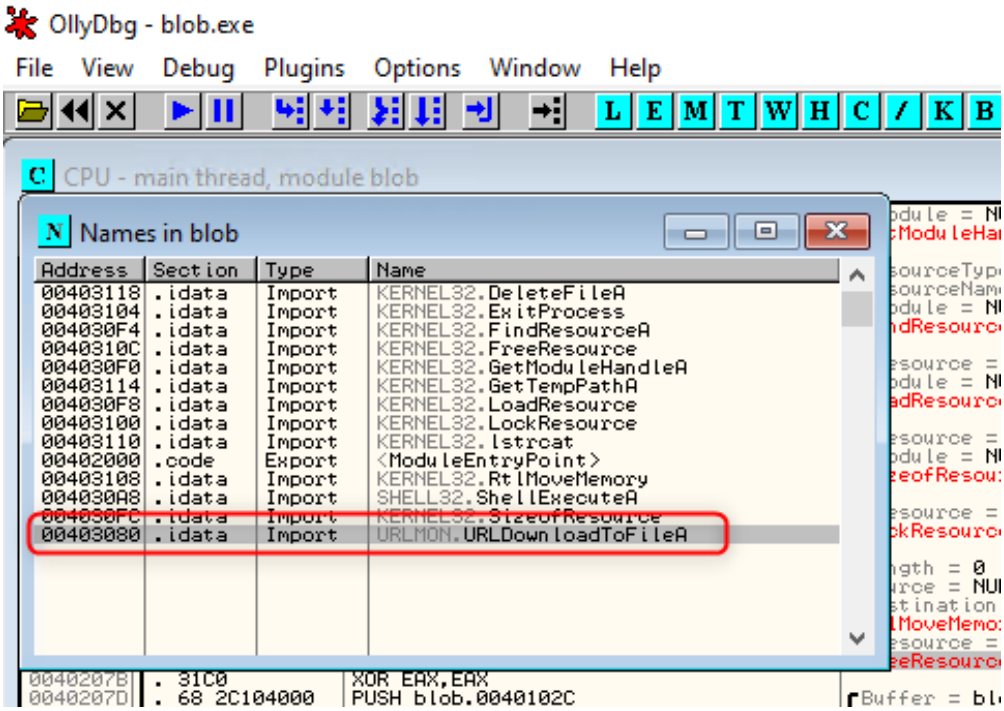


圖 12：該軟體修改編譯日期，顯示編譯時間戳印為 1987 年（資料來源：自測試環境截圖）

2. 惡意程式從哪個網域下載惡意元件？

   答：惡意程式從網域 www 點 o ffs3c 點 com 下載一個 "11111111111111111111111111down1.exe"執行檔（圖 13）。

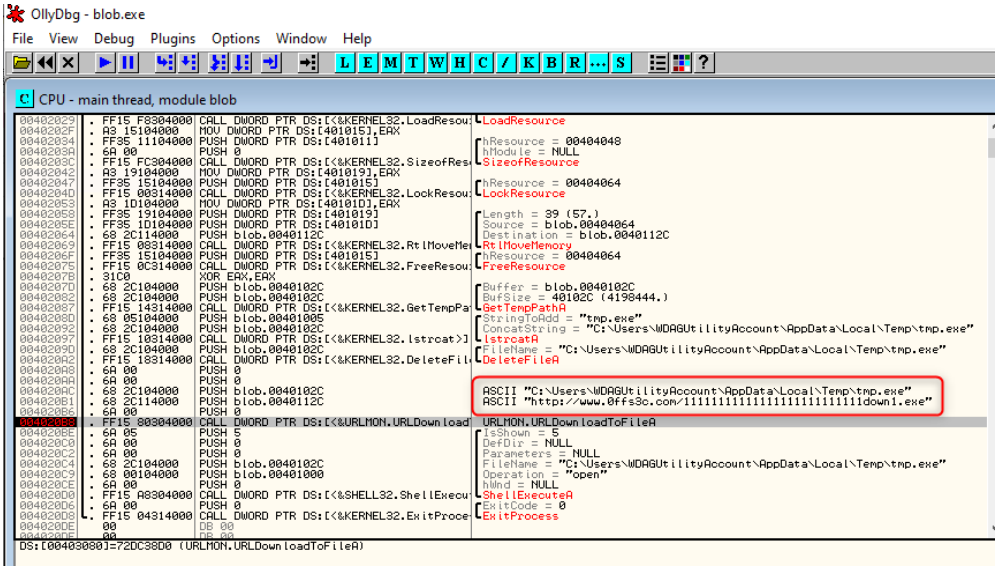


圖 13：惡意程式透過網路下載檔案。（資料來源：自測試環境截圖）

3. 已下載的惡意程式在硬碟上的什麼位置？

答：其下載位置在放在 "%TEMP%" 資料夾下，名稱為 "tmp.exe"（同圖 13）。

(二)分析第二階段則是動態分析，此種分析是透過工具來即時的查看惡意程式的行為、與系統的互動或是網路封包的監聽等情形，課程說明可利用以下工具做不同的行為分析：

1. Process Hacker：用於檢測系統資料和程式屬性，可即時檢視各軟體的 PID、CPU 使用率和狀態等（圖 14）。

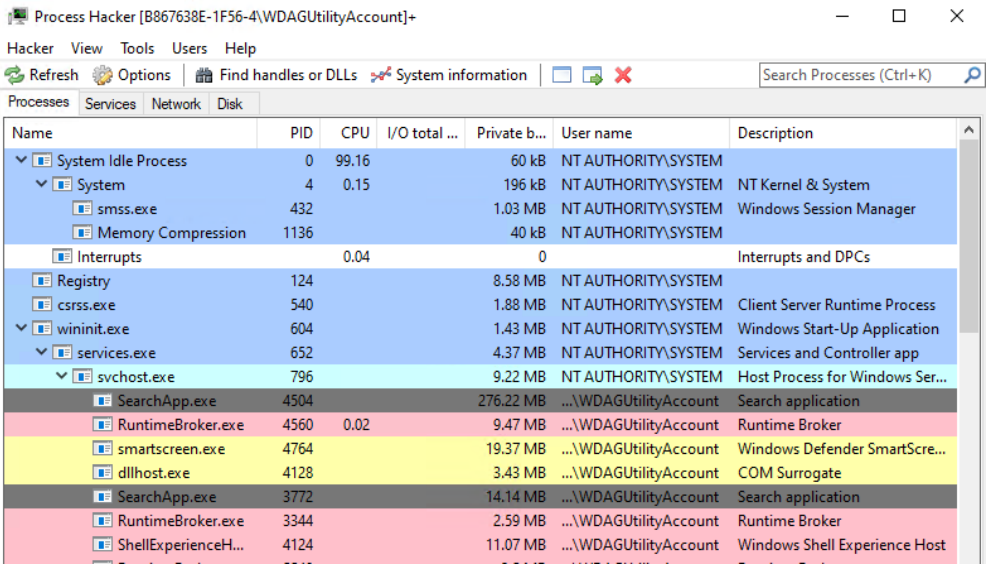


圖 14：呈現目前所有執行中的程式（資料來源：自測試環境截圖）

2. Process Monitor：顯示目前程式與系統之間的即時互動（如檔案系統、註冊表、程序活動），即時檢測時，可利用過濾器減少過多不必要的資訊（圖 15）。

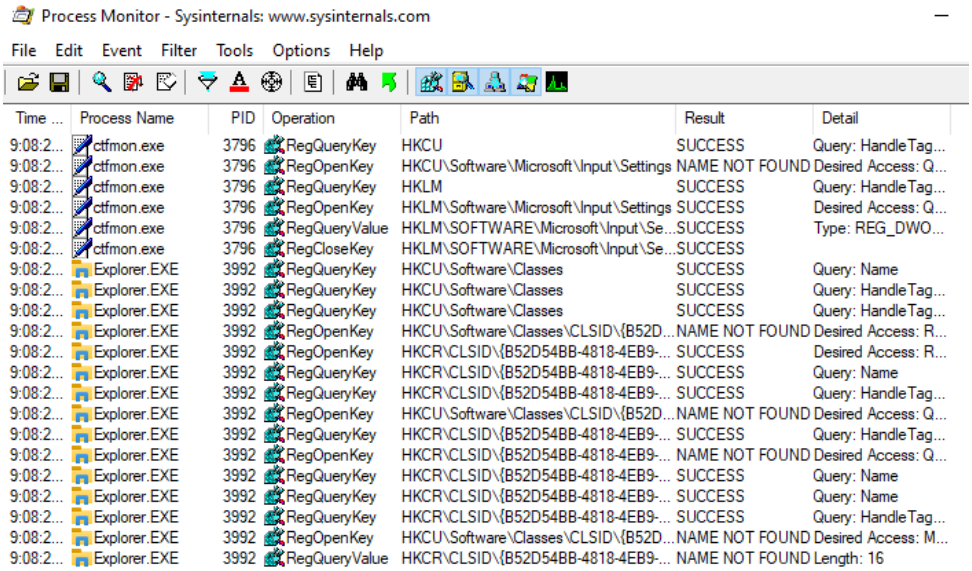


圖 15：各程式正與系統互動的狀態（資料來源：自測試環境截圖）

3. Wireshark：可於執行惡意程式時補捉網路封包，並顯示連線之 IP（圖 16）。

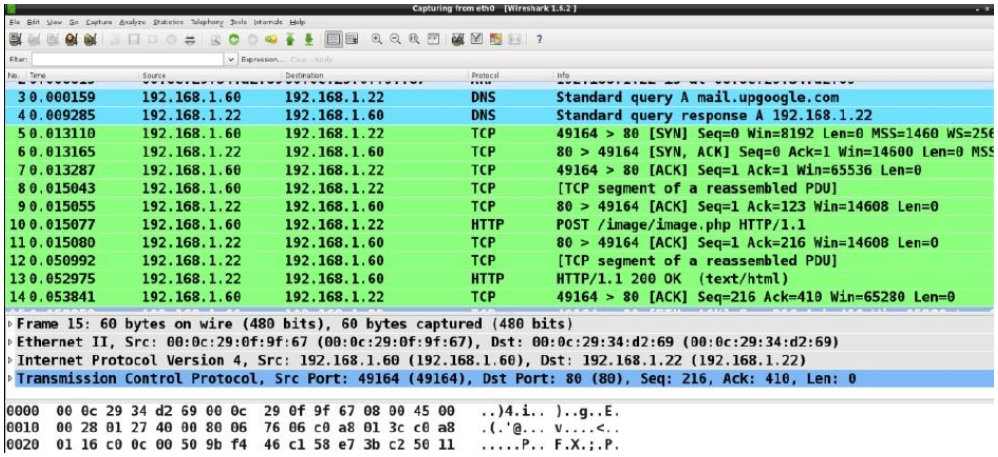


圖 16：顯示所有正在連線的封包（資料來源：講者簡報）

4. Noriben：與 Process Monitor 一起工作的 Python 腳本，用於收集、分析和報告惡意程式的運作情形，並有預設過濾器，有助於分析現況（圖 17）。

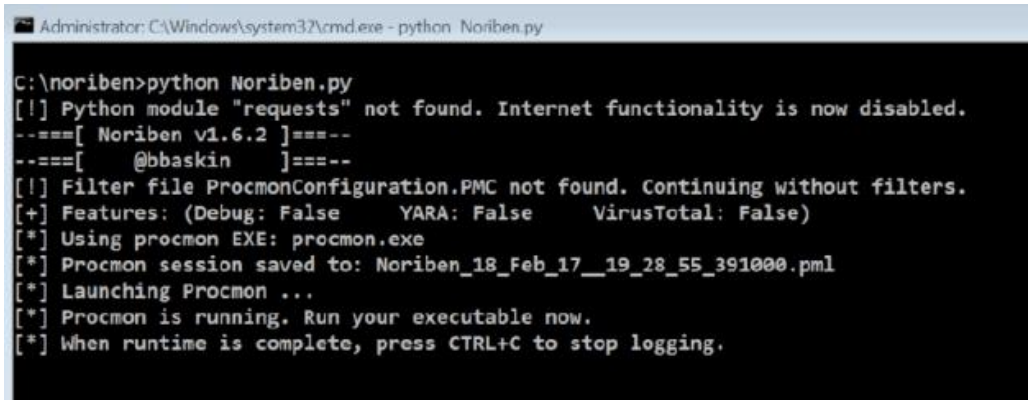


圖 17：顯示 Noriben 正與 Process Monitor 同時執行中（資料來源：講者簡報）

5. FakeDNS：可執行 DNS 服務，並提供虛擬 DNS 回應，可將所有網域解析至本機服務的 IP（圖 18）。

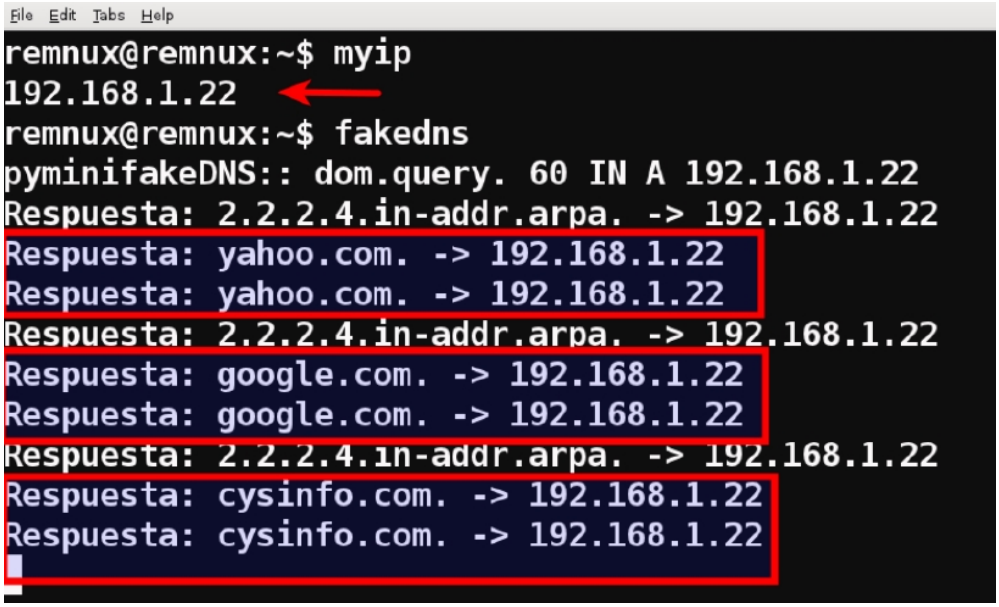


圖 18：顯示 FakeDNS 回應的 IP（資料來源：講者簡報）

6. InetSim：可於實驗室環境中模擬常見的網路服務，並將所有通訊導至系統中，經設定，並可截取網路流量（圖 19）。

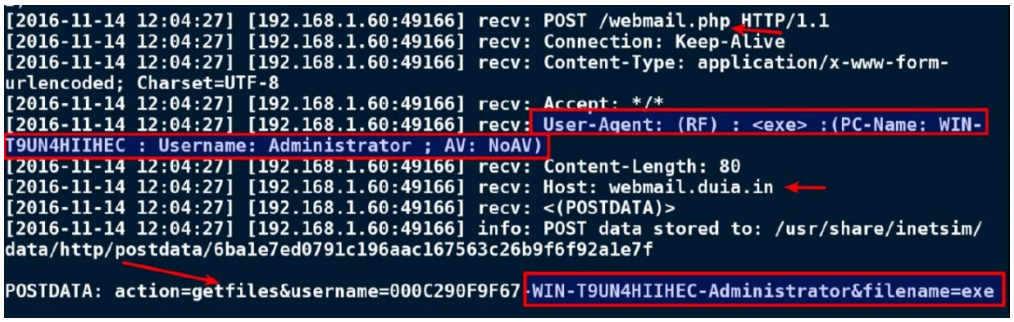


圖 19：顯示 InetSim 截取了 Https 流量（資料來源：講者簡報）

(三)最後記憶體分析的部份，首先介紹程序（process）的概念，程序是執行緒執行管理和控制的物件，於 32 位元作業系統擁有 2GB 或 3GB 或 64 位元作業系統有 8TB 的私人虛擬地址空間（private virtual address speace），並具私人控制代碼表（private handle table），DKOM（Direct Kernel Object Manipulation，直接核心物件操作）和

EPROCESS 之間具有密切的關係，EPROCESS 是 Windows 操作系統中的一個結構，亦代表著每個程序（process），每當一個應用程序或系統服務在 Windows 系統中運作時，操作系統都會為該程序創建一個 EPROCESS 結構來追蹤和管理它的運作狀態。EPROCESS 包含程序許多重要資訊，包括程序 ID、父程序 ID、記憶體佈局、執行緒列表和相關安全設置等。攻擊者使用 DKOM 技術時（圖 20），它們會直接操作 EPROCESS 結構，透過 DKOM 攻擊可欺騙操作系統，使某些程序或惡意活動在 EPROCESS 結構中隱藏或修改其屬性，而避免被傳統的安全防護機制所檢測。

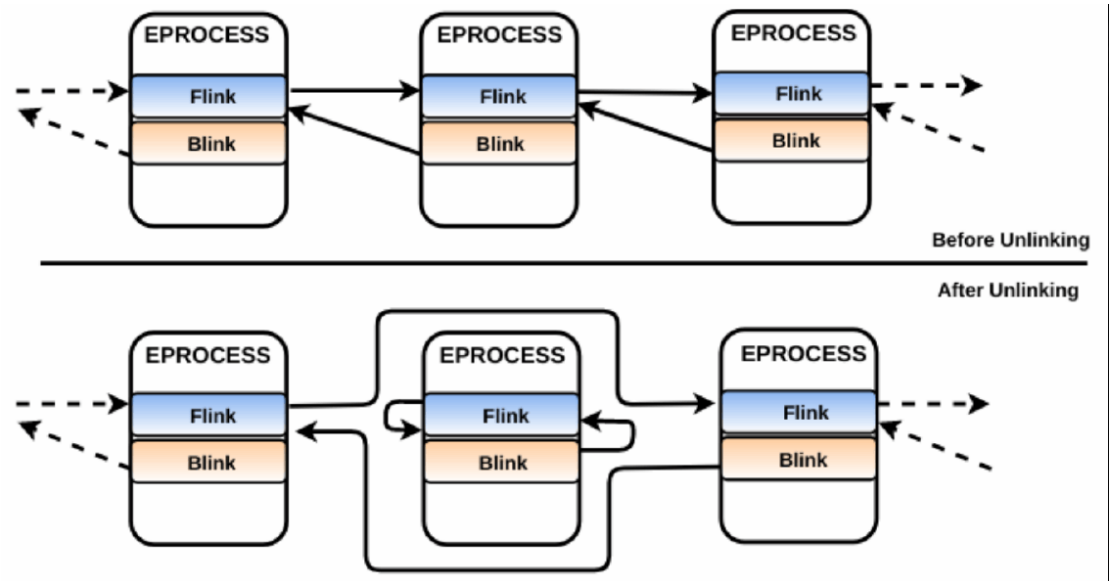


圖 20：DKOM 隱藏某些 EPROCESS 結構使之不易被發現（資料來源：講者簡報）

課程講解基於 Python 開發的 Volatility 工具集中的 vol.py，是用於分析記憶體的工具之一，其有許多參數可使用，每個參數都有不同的功能，以下列出所用到的部份功能：

1. --profile=PROFILE: 指定記憶體映像檔的設定文件，是必備的參數，因 Volatility 需要知道映像檔是來自什麼操作系統，才能根據映像檔的系統和架構進行適當的解析。
2. imageinfo: 顯示記憶體映像檔的基本資訊，如操作系統版本、映像檔大小、位元數等。
3. pslist: 列舉記憶體中的程序，並顯示程序的 ID、名稱、父程序 ID 等。
4. pstree: 以樹狀結構列舉程序之間的層次結構和關聯。
5. handles: 列舉記憶體中的控制代碼，並顯示控制代碼的類型、對應的程序 ID 等。
6. dlllist: 列舉程序加載的 DLL 模組，顯示模組的基底位址、大小、路徑等。
7. --output=dot：可產生 Graphviz DOT 格式檔案，可用於顯示程序與程序之間的關係。
8. connscan：用於分析映像檔中的網路連線功能，可查找記憶體中保存的連線資訊，包含連線 IP、port 和狀態等，有助於查找可疑活動。

課程至此進行了 LAB 模擬實驗，模擬情況如下：組織中的高層主管懷疑他的系統在透過電子郵件收到的附件後受到感染，您是處理此事件的事件回應人員，並已收集了記憶體映像檔（perseus.vmem），請調查該記憶體映像檔。模擬情況提出下列問題，並請學員嘗試於模擬環境下查找解答：

1. 是否看到任何看起來可疑的程序？

   答：經使用指令 python vol.py -f perseus.vmem --profile=Win7SP0x86 pslist，套用 pslist 參數後發現一個可疑的程

序，該程序名稱和正常的 svchost.exe 很接近，但名稱為 svchost..exe，多了一個「.」。

2. 可疑程序的名稱是什麼？

答：「svchost..exe」

3. 可疑程序的 ID 是多少？

答：「svchost..exe」的程序 ID 為 3832。

4. 是否有多個可疑程序？

答：另外亦發現一個程序名稱為「suchost..exe」（正常的程序名為 svchost.exe）（圖 21）。

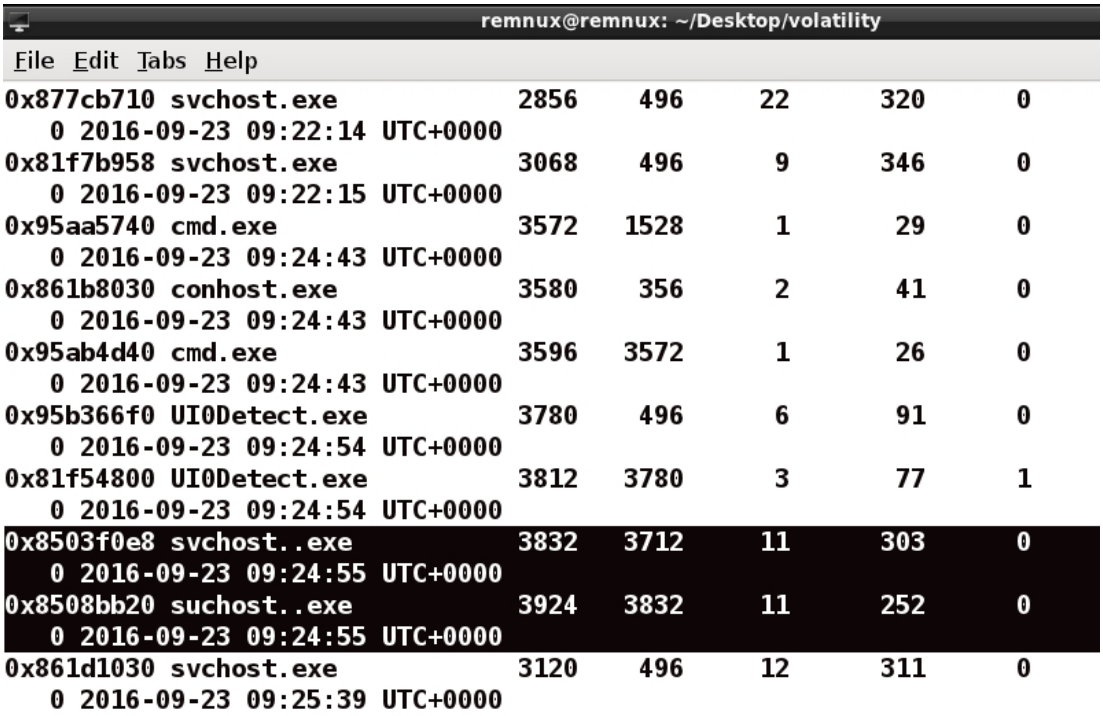


圖 21：於測試環境檢視記憶體映像，並查找出有問題的程序（資料來源：自測試環境截圖）

5. 這些可疑程序之間是否有關聯？

答：兩個程序之間具有關聯性，suchost..exe 的父程序 ID 是 3832，

3832 實屬 svchost..exe 之 ID，表示 svchost..exe 創建了 suchost..exe（程序 ID 3924）。

6. 攻擊者是如何試圖與合法程序混合？

答：攻擊者利用與正常程序名稱極近相似的方式來混肴視聽。

接下來課程開始解說物件和控制代碼（Objects and Handles）的關係，物件管理器（Object Manager）是負責創建和操作物件，並且是靜態結構（static structures）的執行實體（runtime instances），例如：程序、互斥體、事件、桌面、檔案等，物件是存在於核心記憶體中並可透過使用者模式程序來取得物件的控制代碼，而核心程式碼亦能直接取得物件的指標（pointer）或是控制代碼。列舉控制代碼（Enumerating Handles）在 vol.py 中有外掛程式可用-p 選項進行過濾特定程序，用-t 選項則可過濾特定控制代碼類型（圖 22）。

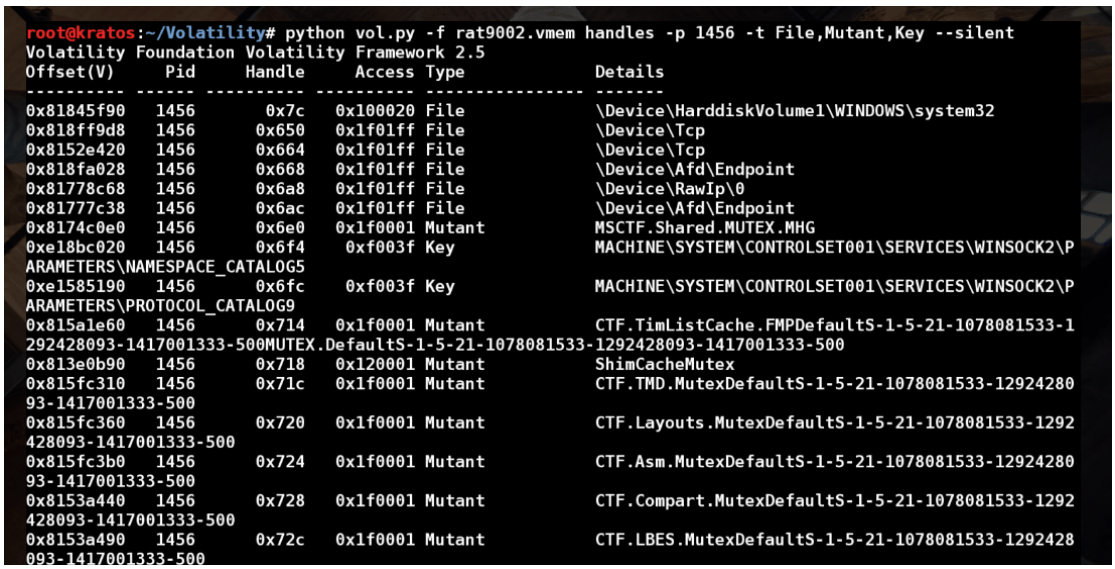


圖 22：指定顯示 PID 1456 所操作的 File、Mutant 和 Key 之控制代碼類型（資料來源：講者簡報）

互斥體（Mutex, 又稱 mutual exclusion 或 Mutant ）是用於同步存取系統上的資源的鎖定機制，為了防止兩個執行緒同時對共享記憶體寫入，每個執行緒在執行存取記憶體的代碼之前等待互斥體物件的所有權，寫入共享記憶體後，執行緒釋放互斥體物件。互斥體通常由惡意程式用來標記其存在並避免受到相同惡意程式的感染，其可視為辨別惡意程式的指標（圖 23）。

```
root@kratos:~/Volatility# python vol.py -f xrat.vmem handles -p 1560 -t Mutant --silent
Volatility Foundation Volatility Framework 2.5
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- --------------- -------
0x816f46e8   1560       0x64   0x1f0001 Mutant          DDrawWindowListMutex
0x817c3f28   1560       0x68   0x1f0001 Mutant          DDrawDriverObjectListMutex
0x816f1218   1560       0x6c   0x110000 Mutant          __DDrawExclMode__
0x818bfc68   1560       0x70   0x110000 Mutant          __DDrawCheckExclMode__
0x8141bde8   1560       0xe8   0x1f0001 Mutant          oZ694XMhk6yxgbTA0
0x81693748   1560       0xec   0x120001 Mutant          ShimCacheMutex
0x817c3ab0   1560      0x160   0x100000 Mutant          _!MSFTHISTORY!_
0x8129cbb0   1560      0x170   0x1f0001 Mutant          c:!documents and settings!administrato
r!local settings!temporary internet files!content.ie5!
0x8143dc50   1560      0x17c   0x1f0001 Mutant          c:!documents and settings!administrato
r!cookies!
0x816c5c38   1560      0x188   0x1f0001 Mutant          c:!documents and settings!administrato
r!local settings!history!history.ie5!
0x817c25d8   1560      0x190   0x100000 Mutant          WininetStartupMutex
0x817c2518   1560      0x1ac   0x100000 Mutant          WininetProxyRegistryMutex
0x814307f8   1560      0x1b0   0x1f0001 Mutant          WininetConnectionMutex
0x817a3248   1560      0x1d4   0x1f0001 Mutant          ZoneAttributeCacheCounterMutex
0x817a3248   1560      0x1d8   0x1f0001 Mutant          ZoneAttributeCacheCounterMutex
0x81513f38   1560      0x218   0x100000 Mutant          RasPbFile
root@kratos:~/Volatility#
```

圖 23：於記憶體映像檔中發現惡意程式標記其存在（資料來源：講者簡報）

註冊表（Registry）是包含 Windows 的各種設定的存在，可作為用於檢測惡意程式是否存在的指標之一，Volatility 的 printkey 外掛可用於列印註冊表的金鑰（key）、子金鑰（subkeys）及其值，惡意程式通常會修改其中一個啟動註冊表金鑰以維持執行（圖 24），以下為常見的啟動註冊表設定位置：

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

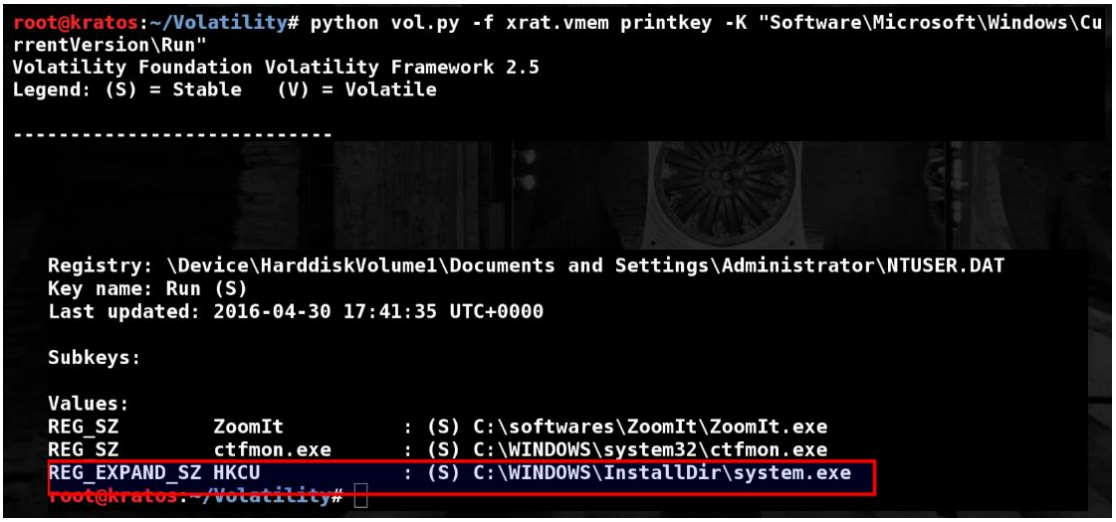


圖 24：發現惡意執行檔"system.exe"被添加到註冊表 Run 的設定中（資料來源：講者簡報）

課程進行 LAB 模擬實驗，模擬情況如下：當你在閱讀有關'spybot'的惡意程式文章時，你發現 spybot 創建了一個互斥體（mutex）"krnel"來標記其存在。分析記憶體映像檔（spybot.vmem）並回答以下問題：

1. 這台主機是否感染了 Spybot？

   答：經使用指令 python vol.py -f spybot.vmem handles -t Mutant |grep -i krnel 確認互斥體的控制代碼顯示了系統上“krnel”的存在，由於這個互斥體與 Spybot 相關，因此系統可能被感染了（圖 25）。

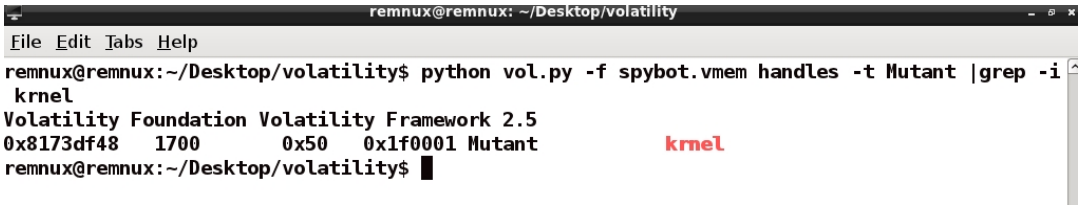


圖 25：於測試環境中辨識出使用 krnel 的存在（資料來源：自測試環境

截圖）

2．惡意程序的程序 ID 是多少？

答：於前次查詢發現其 ID 為 1700。

3．惡意程序的名稱是什麼？

答：經使用指令 python vol.py -f spybot.vmem pslist -p 1700 來查找使用 ID 1700 的程序為「wuaumqr.exe」（圖 26）。

```
remnux@remnux:~/Desktop/volatility$ python vol.py -f spybot.vmem pslist -p 1700
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
                Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ---------
-------------- ------------------------------
0x81754020 wuaumqr.exe            1700   1676      4       37      0      0 2014-10-2
9:32 UTC+0000
remnux@remnux:~/Desktop/volatility$
```

圖 26：於測試環境中查詢並列出 ID 為 1700 的程序（資料來源：自測試環境截圖）

4．與此惡意程序相關的其它程序其 ID 是多少？

答：當執行指令 python vol.py -f spybot.vmem pstree 1700 時，以 pstree 指令列出其餘與 ID1700 相關的程序即發現其父程序名為「scvhost.exe」（正常的程序名為 svchost.exe）（圖 27）。

```
4:49:37 UTC+0000
.. 0x818a1868:csrss.exe                632    380     11    393 2014-06-11 1
4:49:36 UTC+0000
 0x81387710:explorer.exe              1456   1252     15    436 2014-06-11 1
4:49:55 UTC+0000
. 0x8173b850:VMwareUser.exe           1688   1456      8    214 2014-06-11 1
4:49:56 UTC+0000
.. 0x8175a020:scvhost.exe             1676   1688      0 ------ 2014-10-22 1
7:09:32 UTC+0000
... 0x81754020:wuaumqr.exe            1700   1676      4     37 2014-10-22 1
7:09:32 UTC+0000
. 0x81612b28:GrooveMonitor.e          1708   1456      2    108 2014-06-11 1
```

圖 27：於測試環境中查詢與 ID 1700 相的程序（資料來源：自測試環境截圖）

可用指令 python vol.py -f spybot.vmem psscan --output=dot --output-file=spybot.dot 來以將 psscan 結果以 dot 檔產出，可見其呈現與「wuaumqr.exe」相關的樹狀關係圖（圖 28）。

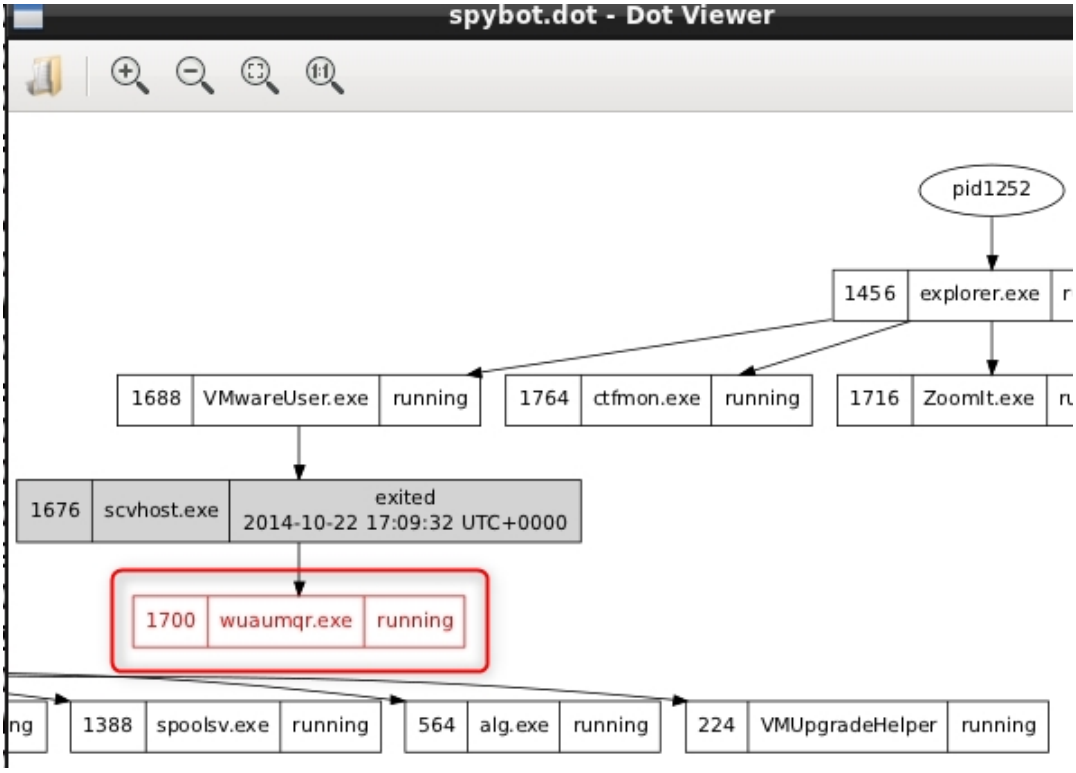


圖 28：於測試環境中查詢與 ID 1700 相的程序（資料來源：自測試環境截圖）

5. 能否識別出 C2 IP 位址？

答：可用指令 python vol.py -f spybot.vmem connscan 將其關聯的網路連線列出，此處可見其使用連線至 209.126.201.22 並使用 6666 port（圖 29）。

```
remnux@remnux:~/Desktop/volatility$ python vol.py -f spybot.vmem connscan
Volatility Foundation Volatility Framework 2.5
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x01949690 192.168.1.100:1033       209.126.201.22:6666       1700
remnux@remnux:~/Desktop/volatility$
```

圖 29：於測試環境中查詢 ID 1700 的連線狀態（資料來源：自測試環境截圖）

二、When Knowledge Graph Meets TTPs: Highly Automated and Adaptive Executable TTP Intelligence for Security Evaluation（當知識圖譜遇上 TTPs：高度自動化和適應性執行 TTP 智能安全評估，講者：Lorin Wu, Porot Mo）

BAS（入侵和攻擊模擬，Breach and Attack Simulation）是一種越來越受重視的安全評估方法。它的目標是模擬攻擊者的 TTPs（戰術、技術和程序，Tactics, Techniques, and Procedures）。在 BAS 中，必須不斷學習攻擊者最新的 TTPs，這對於評估目標組織的安全風險至關重要。同時，需要根據目標組織的實際情況選擇合適的 TTP，以模擬真實的攻擊情境。透過模擬攻擊路徑，我們可以評估目標組織整體的防禦深度，以了解其強項和弱點。

由此可見收集及建立 TTPs 知識庫是極為重要，為此講者於 BAS 安全評估的方法中，提出並創建了一種基於 TTP 導向的新穎知識圖譜方法（圖 30），可以從威脅情報資訊中高度自動化地掌握 TTP 並將其以導入推理引擎的自動調整攻擊鏈。

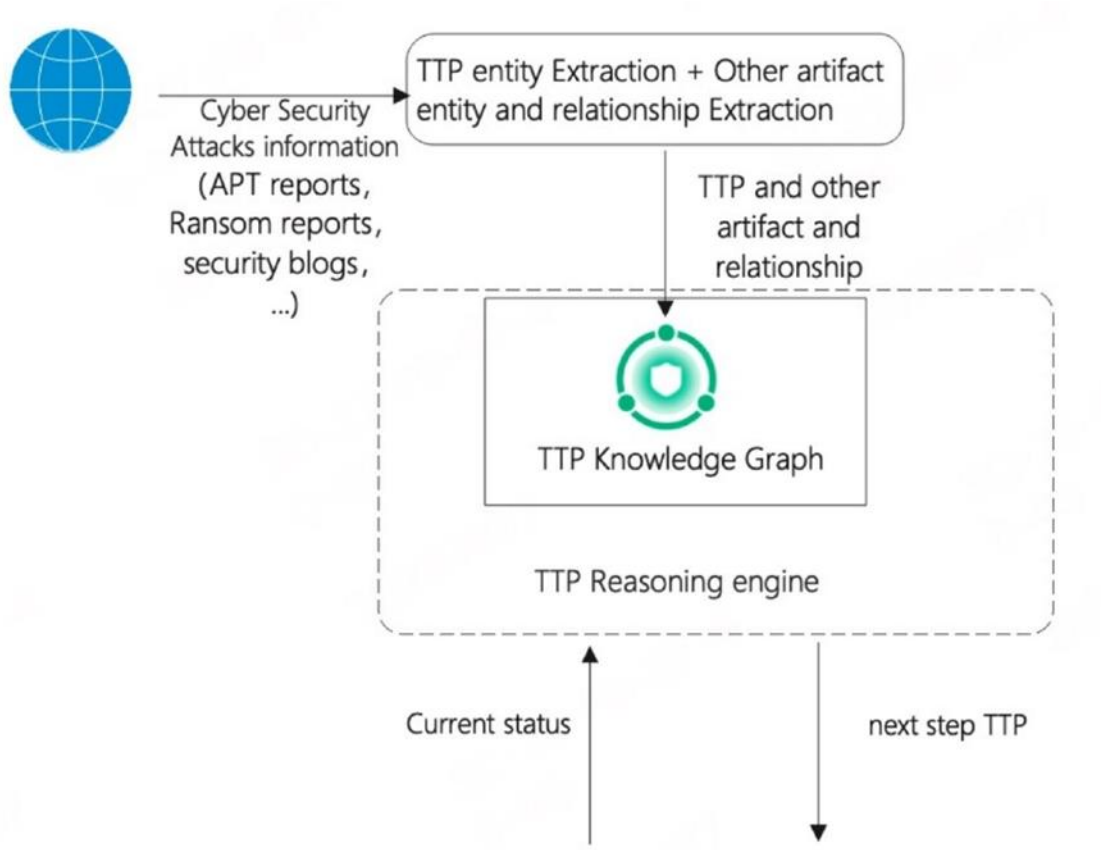
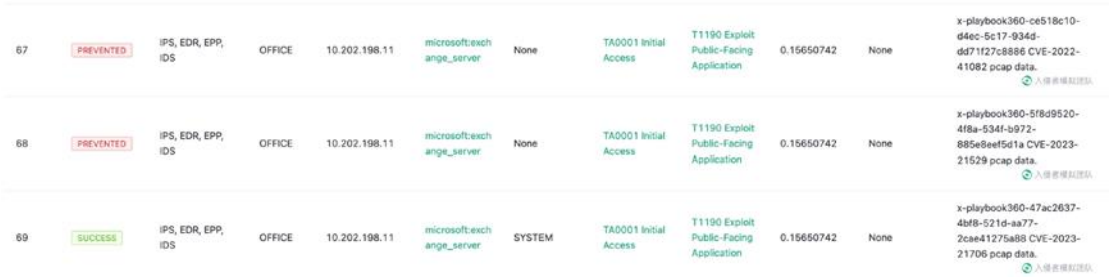


圖 30. TTP 知識圖譜及推理引擎（資料來源：講者簡報）

為了提高 TTP 萃取的準確性，首先需要區分主要和次要的戰術和技術，並根據實際的攻擊場景進行萃取。這包括從命令列、工具和程式碼片段等多個角度萃取參與攻擊的戰術和技術。其次需要根據報告中的攻擊描述上下文進行 TTP 萃取，以獲得更準確的結果。最後則是使用預訓練的語言模型來提升準確性和效率。

而講者採用 TTP 推理引擎是為了以 MITRE ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge，入侵者戰術、技術和共有知識

庫）和權限級別來進行推理攻擊方式，確定攻擊的戰術路徑，通過模擬攻擊的結果，並以主機權限、資產狀態和防禦策略等因素，可以推理出下一步可能使用的技術和程序（圖 31）。



67	PREVENTED	IPS, EDR, EPP, IDS	OFFICE	10.202.198.11	microsoft:exchange_server	None	TA0001 Initial Access	T1190 Exploit Public-Facing Application	0.15650742	None	x-playbook360-ce518c10-d4ec-5c17-934d-dd71f27c8886 CVE-2022-41082 pcap data.
68	PREVENTED	IPS, EDR, EPP, IDS	OFFICE	10.202.198.11	microsoft:exchange_server	None	TA0001 Initial Access	T1190 Exploit Public-Facing Application	0.15650742	None	x-playbook360-5f8d9520-4f8a-534f-b972-885e8eef5d1a CVE-2023-21529 pcap data.
69	SUCCESS	IPS, EDR, EPP, IDS	OFFICE	10.202.198.11	microsoft:exchange_server	SYSTEM	TA0001 Initial Access	T1190 Exploit Public-Facing Application	0.15650742	None	x-playbook360-47ac2637-4bf8-521d-aa77-2cae41275a88 CVE-2023-21706 pcap data.

圖 31．系統自動切換攻擊手法並逐漸提升權限（資料來源：講者簡報）

講者的 BAS 系統使用了多種技術和工具並且運用了混合規則引擎及邏輯編程引擎。這些技術和工具的結合確保了系統的高效運行和快速的推理速度，並依受攻擊系統之回應進行推理而轉換攻擊模式，實際展現現今智慧技術的結晶。

綜上所述，BAS 在當今複雜的安全環境中扮演著關鍵的角色。它通過模擬攻擊和評估防禦策略的完整性，幫助組織提前發現並解決安全漏洞。通過不斷學習攻擊者的戰術、技術和程序，使系統管理者能持續挖掘問題所在，並提升系統安全防禦能力。

三、Operation Clairvoyance: How APT Groups Spy on the Media Industry（千里眼行動：APT 組織如何監視媒體行業，講者：Yue-Tien Chen ,Zih-Cing Liao）

講者演講重點在於關注 APT 族群針對臺灣媒體公司的針對性攻擊並將這一系列攻擊稱為「千里眼行動」，網路間諜行動者持續對媒體業表現出極大的興趣，這些行動者喜歡通過這些媒體公司和記者的「眼睛」觀察臺灣的日常活動。在 2022 年，臺灣局勢更顯嚴峻，講者觀察到越來越多的進階持續性威脅（Advanced Persistent Threat, APT）族群滲透到臺灣的媒體業。根據觀察，媒體業已成為這些 APT 組織的第一個非政府組織類型的攻擊目標。

而媒體業所面臨的 APT 攻擊主要來自於以下方面：郵件攻擊、過時的硬體和軟體、社交媒體攻擊、資訊安全人員以及網路服務的弱點。講者提出各 APT 組織皆有其特定的攻擊手段，其中的一個例子是 CloudDragon（又稱為 Kimsuky）組織，它的目標國家包括韓國、日本和美國。他們使用各種技術和策略來進行攻擊，慣用手法有釣魚攻擊和 BabyShark 惡意軟體攻擊，以此來入侵和監控目標機構的資訊系統。

臺灣的媒體業成為了 APT 攻擊的目標，由於臺灣的地緣政治地位、選舉過程和半導體產業的重要性。每當有特別的政治活動時，即可能會成為攻擊發起的時間點(圖 32)，例如，當美國眾議院訪問臺灣時，臺灣的部分數位廣告看板和 YouTube 頻道即受到了入侵。

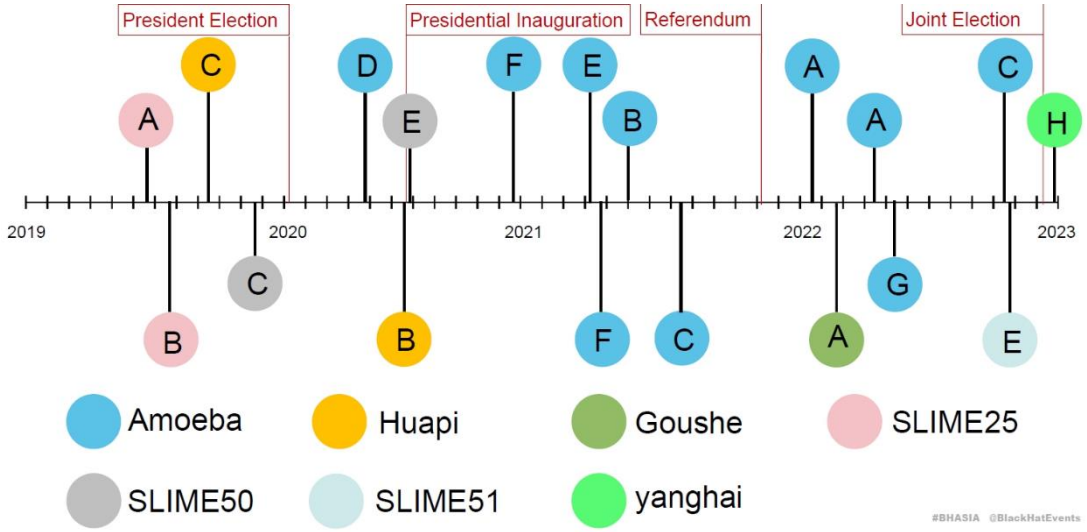


圖 32. APT 組織攻擊時間點（資料來源：講者簡報）

而千里眼行動是一個特定針對臺灣媒體的 APT 攻擊活動。這個行動涉及到多個 APT 組織，包括 Amoeba、Huapi、Goushe、SLIME25、SLIME50、SLIME51 和 yanghai(圖 33)。這些組織在過去幾年中對臺灣媒體發動了多次攻擊，這些攻擊的時間軸可以追溯到 2019 年至 2023 年。它們使用的手法包括釣魚攻擊、惡意軟體傳播、社交工程和供應鏈攻擊(一種傳播間諜軟體的方式，一般通過產品軟體官網或軟體包存儲庫進行傳播)等。APT 組織往往將攻擊行動分為多個階段，包括入侵目標網路、執行惡意程式碼、探索內部網路、竊取敏感資料和進行長期監控等。

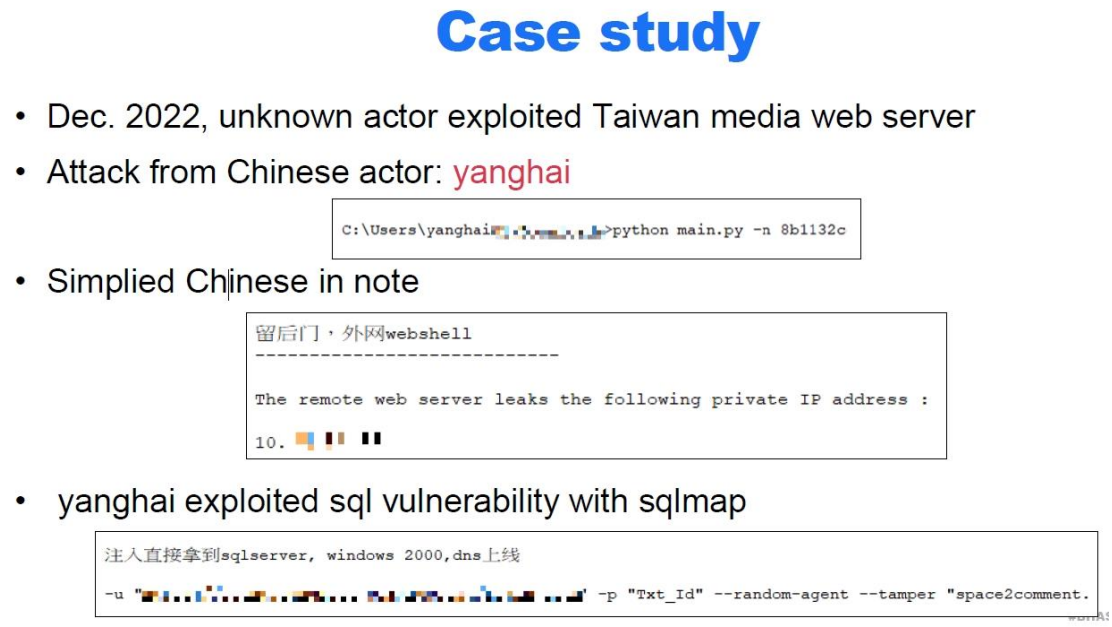


圖 33. 講者展示 yanghai 部份攻擊語法及註解（資料來源：講者簡報）

為了應對這些 APT 攻擊，講者建議媒體機構需要實施一系列的安全措施。首先，加強員工的安全意識培訓，使他們能夠識別和應對釣魚郵件、惡意連結和可疑附件。其次，加強網路安全，包括使用強大的密碼、定期更新軟體和防火牆的使用。同時，媒體機構應該實施嚴格的訪問控制和權限管理，確保只有授權人員能夠訪問敏感資料。

此外，講者建議應加強法律和法規的制定，政府應該加強監管措施，確保媒體機構能夠適應 APT 攻擊的快速演變。同時，加強對 APT 攻擊的打擊力度，將攻擊者追究到法律責任，為受害者提供保護和補償。

四、Dirty Stream Attack, Turning Android Share Targets Into Attack Vectors（惡意串流攻擊：將 Android 共享目標轉化為攻擊向量，講者：Dimitrios Valsamaras）

Android 作業系統提供了一種稱為 intent(意圖)的方便機制，可用於在 APP 之間共享數據和檔案。然而，如果沒有正確的使用，這種功能也會帶來潛在的安全漏洞。其中一種漏洞稱為惡意串流攻擊(Dirty Stream Attack)，它利用 APP 對接收進來的串流盲目信任，並且未進行適當的驗證，進而成功取得資訊。

在惡意串流攻擊中，惡意的 APP 利用特製的內容攜帶 payload(酬載)並將其發送到目標 APP(圖 34)。如果接收方未執行必要的安全檢查，攻擊者可透過特製內容和串流，來將將惡意內容覆蓋到關鍵文件中。此外，在某些條件下，可能還會讓接收方受保護的文件被複製到公共目錄中，使用者的私人數據因此面臨巨大風險，這種攻擊可能產生嚴重後果，尤其是當具有數百萬安裝的熱門 APP 有此漏洞時。為了降低風險，實施安全措施是至關重要的。

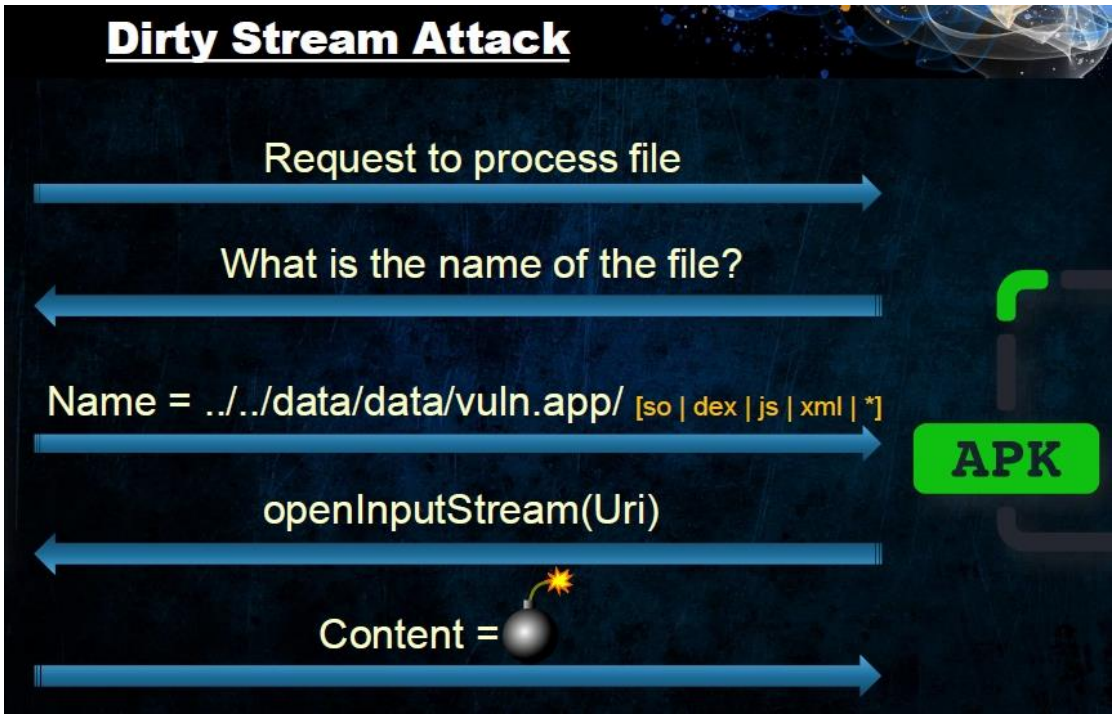


圖 34. 惡意串流攻擊來自惡意程式（資料來源：講者簡報）

以下是講者建議措施：

1. 下載應用程式時要注意：在下載應用程式時，應僅從信任的來源（例如 Google Play Store）下載 APP，永遠不要從不受信任的來源安裝 APP，避免從未知或不受信任的第三方網站下載應用程式，以減少受到潛在的惡意應用程式的風險。
2. 安裝更新和修補程式：即時安裝應用程式的更新和修補程式，以確保您的 APP 具有最新的版本。
3. 審查權限要求：在安裝應用程式時，仔細審查應用程式對權限的要求。如果一個應用程式要求過多或不必要的權限，請懷疑其安全性。

當我們意識到存在這種漏洞並發現受其影響的應用程式時，講者建議立即與供應商聯繫，亦可提供相應的修復方案，使每個使用者都能致力於維護一個安全的 APP 生態系統。總知，惡意串流攻擊是一種嚴重的安全漏洞，可能導致用戶數據的損失和風險。開發人員和用戶都應該加強對這種攻擊的警覺，並採取相應的防禦措施，包括實施安全措施和注意應用程式的來源和權限。只有通過合作和共同努力，才能確保 Android 應用程式的安全性和用戶的隱私。

五、Insider Threats Packing Their Bags With Corporate Data（將企業數據打包的內部威脅，講者：Dagmawi Mulugeta ，Colin Estep）

內部威脅和資料外洩是企業所面臨的重要風險之一，內部威脅指的是企業內部的員工或合作夥伴，可能有意或無意地對企業的資訊進行濫用、竊取或外洩的行為。這種行為可能對企業的機密資料、知識產權、客戶數據以及企業聲譽帶來嚴重的損害。因此，組織應該重視並制定相應的措施來防範這些風險。

根據 2020 年的 Securonix 內部威脅報告，內部威脅中的一個重要類別是「離職風險」員工，據調查結果，有 60%的內部威脅涉及此類員工，這意味每個組織都有可能存在潛在此風險。

資料外洩是內部威脅中的一個主要行為，是指將敏感的企業資料通過各種方式進行非授權的外部洩露。這些資料可能包括知識產權、個人身份資訊（PII，Personally Identifiable Information）、商業機密等。根據講者調查，有 15%的離職風險員工將數據移至個人 APP 而使資料外洩，而 85%的離職風險員工則無此舉。值得注意的是，大多數數據外洩行為發生在離職前的最後 50 天內，這顯示了在這個時間段內加強對數據外洩的監測和防範的重要性。

為了檢測和防範內部威脅和數據外洩，組織應該制定相應的策略和措施。講者提到的一種解決方案是透過監測和異常檢測工具。這些工具可以監測雲端流量、應用程序的使用情況，並對資料移動的量、性質和方向進行分析，以檢測異常行為和數據外洩的跡象。例如，通過異常檢測，可以發現使用者行為的變化，並通過資料標籤和資料損失防護（DLP）技術來識別和保護敏感檔案(圖 35)。

User	App	App Instance label	Activity	File Name	DLP Violation
dagmawi@gmail.com	Google Drive	personal	upload	black_project.docx	Secret project code names

圖 35.資料標籤紀錄（資料來源：講者簡報）

此外，簡報中還提到了幾個數據統計結果，這些結果可以幫助組織更好地了解和應對內部威脅和數據外洩的風險。根據講者簡報中的數據(圖 36)，共有 207 個組織、調查了 470 萬活躍用戶，從這些組織的數據中可以看出在離職前的最後 50 天內，有相當一部分的數據被 2%的人員通過雲端應用程式外洩了企業資料，然而，這 2%的外洩行為涉及到的資料主要是知識產權和個人身份資料，這可能對企業造成重大損失。

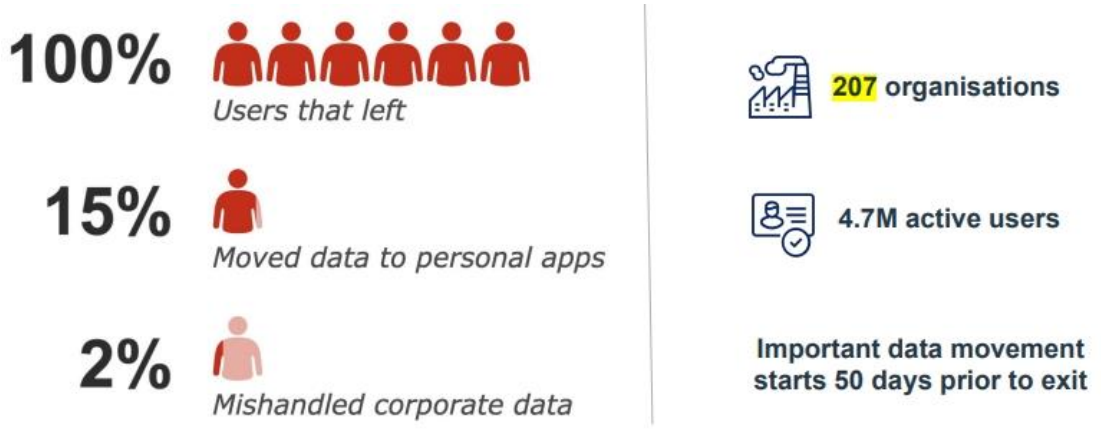


圖 36. 調查資料，離職前 50 天行為（資料來源：講者簡報）

最後講者提到，內部威脅和數據外洩是企業所面臨的重要風險，需要組織重視和有效應對。組織應該制定內部安全策略，運用監測和異常檢測工具，並加強對數據移動的監測，以及數據標籤和數據損失防護技術的應用。這樣可以提高對內部威脅和數據外洩的檢測和預防能力，保護企業的敏感資訊和利益。

六、Leveraging Streaming-Based Outlier Detection and SliceLine to Stop Heavily Distributed Bot Attacks（利用基於串流的異常檢測和 SliceLine 來阻止大規模分佈式機器人攻擊，講者：Antoine Vastel, Konstantina Kontoudi）

目前我們使用 CAPTCHA 做為驗證技術之一，是因為有各種被惡意使用的 bots(機器人程式)去攻擊各式網頁而產生的驗證方式，至於要如何去偵測一個惡意使用的 bots 並且不使用 CAPTCHA 驗證呢？講者提出使用基於串流型式的異常檢測及 SliceLine(是種是用來尋找資料的除錯技術模型，為一種 Python 函式庫)來阻止大規模分散式機器人攻擊，簡報中提到使用 Python 開源技術來搭

配運作 SliceLine，展示攻擊者利用成千上萬個被感染的 IP，並繞過傳統的安全機制進行攻擊，而如何應用於特定且困難的機器人檢測子集如速率限制策略來阻止攻擊(圖 37)。

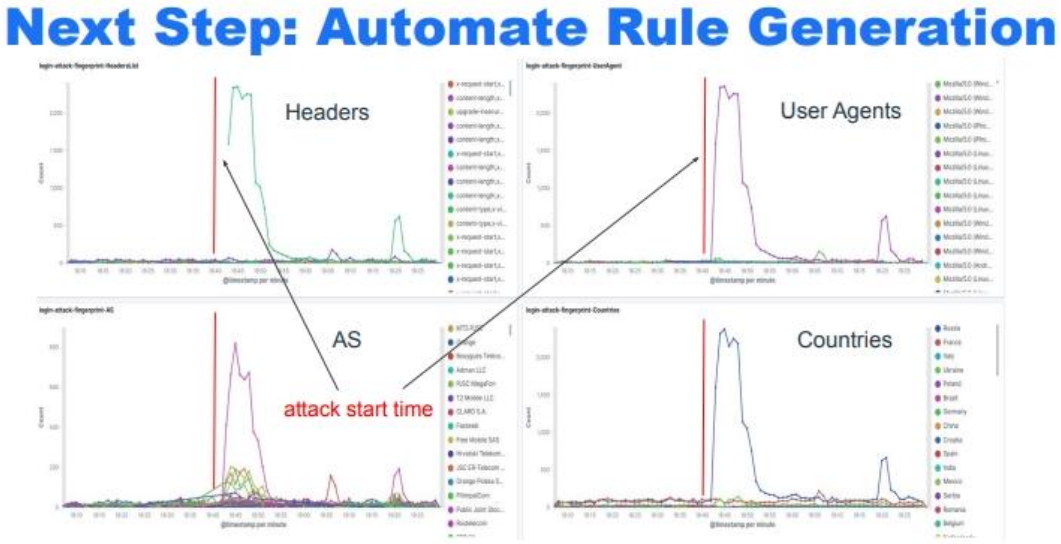


圖 37. 攻擊開始後於可疑流量中開始分析（資料來源：講者簡報）

SliceLine 最初是設計用於辨別機器學習模型表現不佳的數據子集，但其可用於生成大量與攻擊相關聯而不帶有標籤數據的功能，被講者利用來檢測 bots 問題，並說明如何使用 SliceLine 即時模擬生成大量的惡意簽證，計算模型預測值與實際值之間的差異來評估數據子集的表現，利用矩陣運算的高效性，快速計算出不同子集的差異程度，從而找出表現不佳的子集。這使得開發人員可以專注於那些需要改進的數據，並針對性地進行調整，以提高整體模型的性能。

於簡報後半段，講者介紹針對 SliceLine 最佳化的 Python 程式碼，並展示了它在一個難度較高的機器人檢測子集中的應用，詳細說明如何使用串流式檢測來發現分散式攻擊，並利用數據建模和 SliceLine 技術來辨別攻擊並生成相

關的規則。其中還分享了一個真實案例，並於去年使用這種方法成功阻止了超過 2.85 億次惡意登錄嘗試(圖 38)。

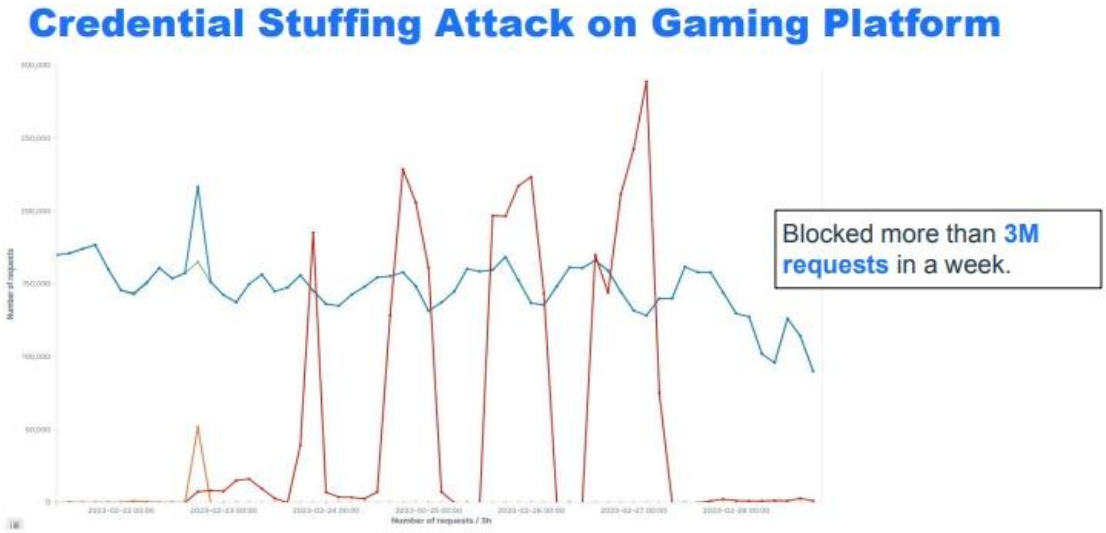


圖 38.一星期中偵測到數次大規模攻擊（資料來源：講者簡報）

講者提供了一個全面的視角，展示如何利用串流式異常檢測和 SliceLine 技術來阻止攻擊和惡意流量。演示從介紹 bots 的定義和惡意用途開始，探討了不同類型的機器人攻擊，包括憑證填充、DDoS、卡片盜刷和投票操縱等，以此提供了一個綜合的解決方案，幫助用戶更好地理解和應對 bots 攻擊，並展示了一種創新的方法來快速生成大量阻止惡意流量的規則。這對於保護網絡安全和防止惡意行為具有重要意義。

七、Sweet Dreams: Abusing Sleep Mode to Break Wi-Fi Encryption and Disrupt WPA2/3 Networks（甜美夢境：濫用睡眠模式破解 Wi-Fi 加密並干擾 WPA2/3 網路，講者：Mathy Vanhoef, Domien Schepers）

Wi-Fi 技術的發展使得無線網路連接變得廣泛且便利。然而在早期的安全協議 WEP 迅速就被破解而存在嚴重漏洞，極易受到攻擊，後來引入的 WPA1/2 協議提供了更強的安全性，但仍存在離線密碼暴力破解等漏洞。近年來，作為新一代 Wi-Fi 安全協議 WPA3 被設計出來，增加了更多的安全改進，而在 2018 年，WPA3 也被發現存在一些安全漏洞如被稱為 Dragonblood 的旁路攻擊。Wi-Fi 安全一直是不斷發展的領域，需要持續的研究和改進來保護用戶數據和隱私。

講者介紹了三種濫用 Wi-Fi 的睡眠（省電）功能的新型攻擊。在第一種攻擊中，針對一個受保護的 Wi-Fi 網路，濫用睡眠模式使其以明文方式洩露訊框，其思路是攻擊者發出睡眠的通知給 AP(無線基地台,Access Point)，進而使該 AP 進入緩衝模式，然後再發出認證連線，迫使移除配對金鑰，導致暫存的訊框使用錯誤或無金鑰的方式進行傳輸，進而使資訊外洩(圖 40)，訊框洩漏的方式會因不同的核心(kernel)而有些不同，這種核心洩漏連 Linux、FreeBSD 和 NetBSD 的軔體亦受影響。

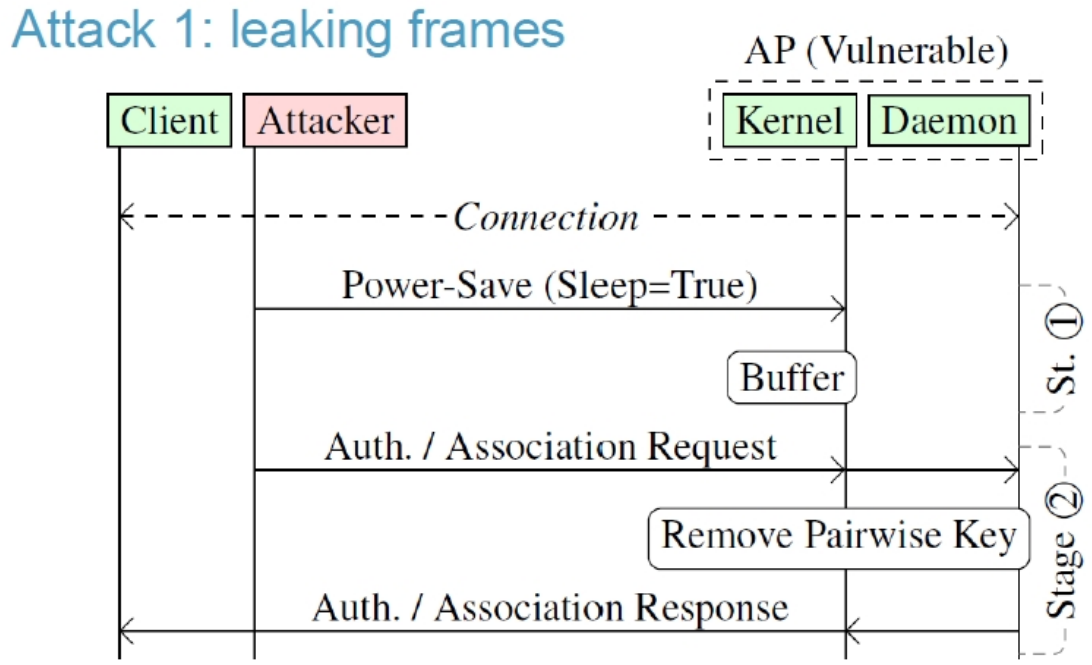


圖 40. 攻擊模式的階段狀態（資料來源：講者簡報）

在第二種攻擊中，講者提出一種繞過 MFP(訊框保護管理，Management Frame Protection)的 DOS(阻斷服務)攻擊方式，並展示這種攻擊的模式，攻擊者透過發出仿造的連線協議請求，其中包含了睡眠的設定值，雖然 AP 會退回請求，但此時 AP 想再發出確認訊息來確認真正用戶端是否還存在線，但卻被核心層以為該連線已進入睡眠模式而將該確認訊息存入暫存區不發出，最後使該用真實用戶被中斷連線(圖 41)。即使啟用了 WPA3 和受保護的管理訊框，攻擊也可以用於斷開客戶端的連接。

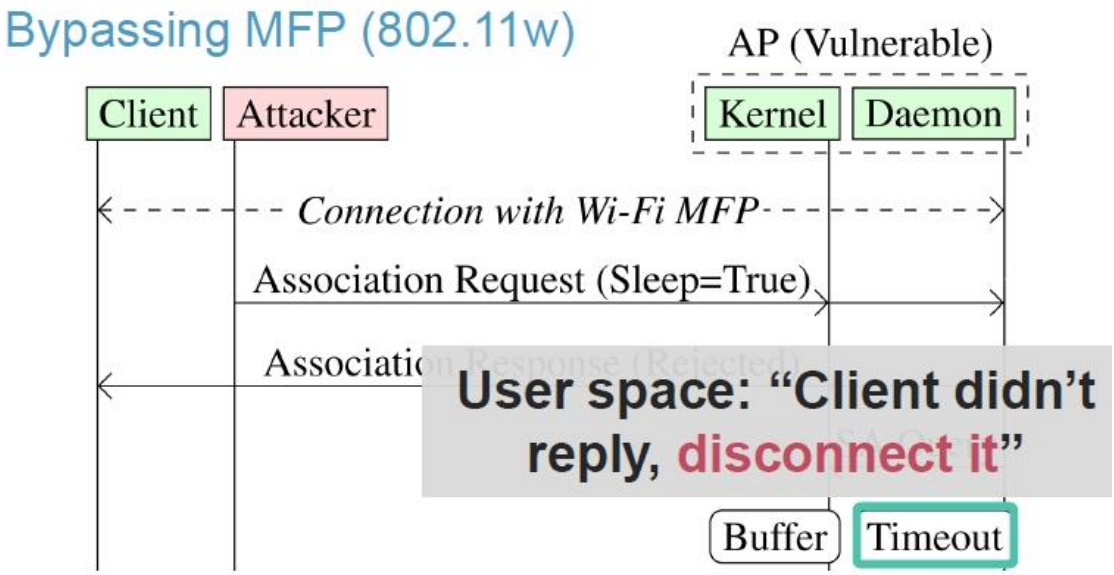


圖 41.攻擊模式的階段狀態（資料來源：講者簡報）

第三種攻擊模式，講者表示可於繞過用戶端隔離模式(Client isolation bypass)，其原理是發出 DNS 請求後，馬上偽造用戶端的 MAC Address，並與 AP 連線取得新的加密金鑰，即可等待接受從外面回傳回來的 DNS 回應，進而可能洩漏部份資訊(圖 42)。

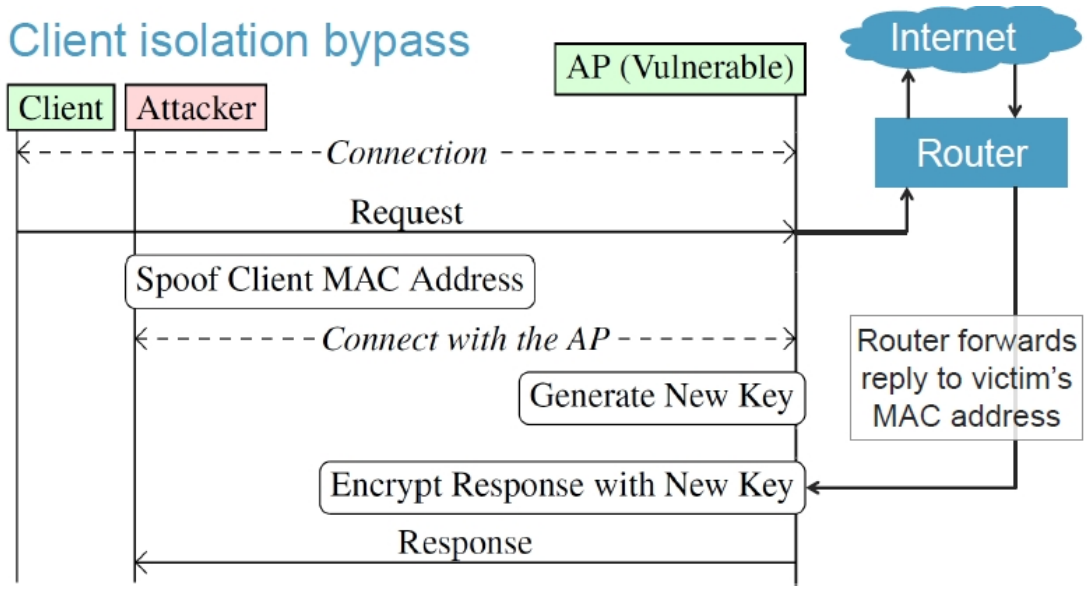


圖 42.攻擊模式的階段狀態（資料來源：講者簡報）

這些攻擊展示了 Wi-Fi 安全的脆弱性，講者強調了持續研究和改進的重要性，以保護用戶數據和隱私，同時，使用者和供應商都應該採取適當的安全措施，來確保 Wi-Fi 網路的安全性。

八、Security advocacy shouldn't be for security professionals: an analysis of how the industry misses the mark and how we can improve（安全倡議不應僅針對安全專業人士：分析行業的不足之處以及我們如何改進，講者：Sarah Young）

在課堂中，講者提到在傳統上，資安專業人士在產出各種資安相關的內容如文件、培訓資料、影片、部落格文章和 Podcast(類似網路電台節目)等內容時，通常只針對資安專業人士撰寫，這在業界內很常見，但資訊安全對每個人

十分重要的，而這些內容並未以大眾的角度來編寫，因此很難被廣泛接受和實施。

現今的資安專業人士，常常陷入幾個常見的問題，如他們知道的知識越多，解釋事件的能力就越差，又或是常以假定受眾皆已有相關知識而忽略解釋，這導致資安資訊更不易普及。講者經由分析超過 200 則以上的資安內容，其中內容比例包含 36%的影片、13%的培訓課程、33%的文件、7%的書籍和 11%的 potcast，而創作來源是來自內容創作者、供應商和非營利組織等三大類，以非營利組織所產出的內容反而是更容易讓人理解和接受的(圖 43)。

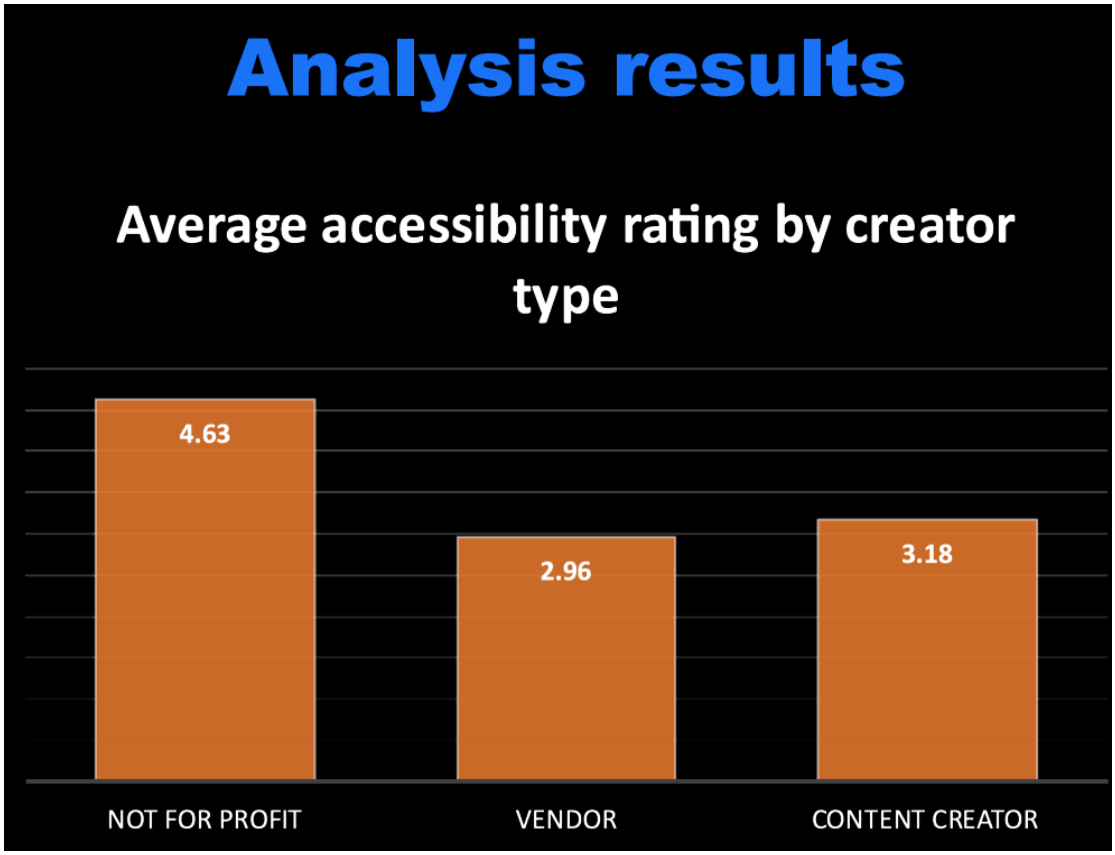


圖 43.創作者易用性評分（資料來源：講者簡報）

此舉不僅讓人思考資安相關內容究竟出了什麼問題？是任何人都能消化這個內容並開始執行嗎？還是這個內容產出是出自於什麼目的？又或是這些內容有明確的開始、中間和結尾，或是過於冗長？基於這些問題，TL;DR（太長沒時

間讀，too long, didn’t read）的原則應運而生，這種縮寫表示內容過於冗長或難以理解。

講者建議我們應該以 TL;DR 的原則來思考資安相關內容。鑑於這些內容並非大多數人可以理解的方式撰寫，我們應該改變資安內容的呈現和解釋方式。我們不應該害怕給出明確的指示，而是應該詢問非資安專業人士的意見，以問自己「我的媽媽能理解這個嗎？」的這種方式來確保內容是否易於使用。

總結來說，講者建議組織內的資安相關內容應該檢查是否能夠提供簡單明確的指導，使非安全人員也能夠遵循。同時，根據 TL;DR 的原則，創建摘要或明確的步驟，使資安人員更容易按照指示完整執行，並大幅降低資安漏洞的風險。這樣的改變將使資安推廣更加親近和可行，讓更多人能夠參與到資訊安全的範疇中。

九、A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks（每天慢跑無法阻止駭客：對健身追踪社交網路中終端隱私區域的推論攻擊，講者：Karel Dhondt, Victor Le Pochat）

講者於簡報中表示健身追蹤社交網路（如 Strava）此類允許使用者記錄運動活動並公開分享的網路服務，原意是為了鼓勵人們分享互動，但卻同時存在隱私風險，因為活動的起點或終點可能無意中暴露了個人隱私的位置，如住家或工作場所的精確地點，為了降低這種風險，健身追蹤社交網路引入了端點隱私區域（EPZ，Endpoint Privacy Zones）技術，該功能可以隱藏受保護位置周圍的活動軌跡部分，希望能減少被發現的可能性。雖然健身追蹤社交網路中的

端點隱私區域（EPZ，Endpoint Privacy Zones）功能可遮蔽該地點一定的範圍(圖 44)，以期望降低被發現的可能，但仍存在受推論攻擊的一定風險性。

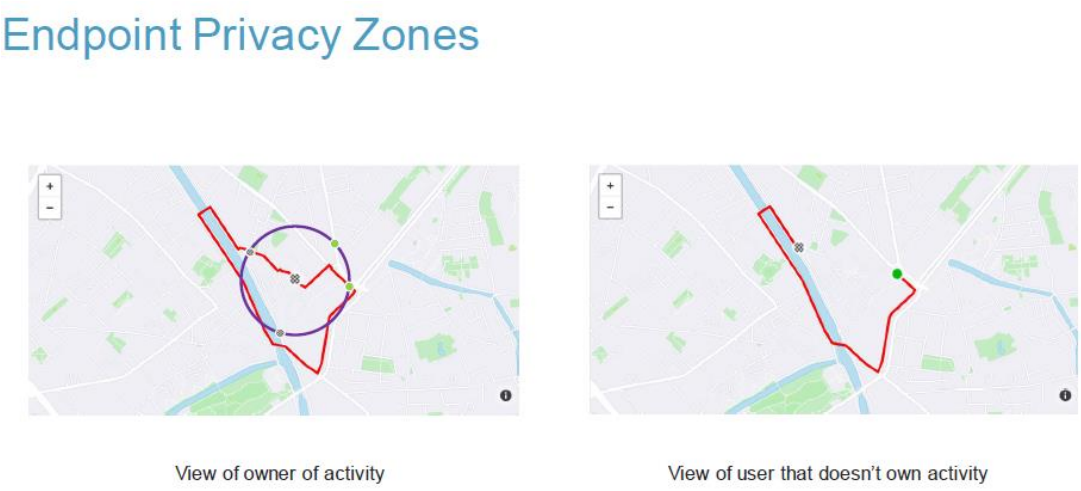


圖 44. 使用者本人可見活動範圍及非本人可見活動範圍(已啟用 EPZ) （資料來源：講者簡報）

健身追蹤社交網路原先為了降低隱私風險，而引入端點隱私區域（EPZ）技術，該功能可以隱藏受保護位置周圍的活動軌跡部分，然而，講者研究發現端點隱私區域仍然容易受到推論攻擊，這些攻擊可以明顯降低該功能提供的隱匿性，甚至可推算出受保護的位置。攻擊者利用活動數據中所顯示的總活動距離資訊，及街道脈絡數據以及進出端點隱私區域的位置，從而獲得一個可推論的空間，並利用迴歸分析來預測受保護位置。

講者所用之推論攻擊採用了數個攻擊方法，如利用預先處理步驟推算出保護範圍中的所有路徑及節點、辨識門口、過濾異常值及位置推論等，以綜合結果來推導出可能性最高的位置(圖 45)。

圖 45．程式推論出可能性最高之地點（資料來源：講者簡報）

針對此類的攻擊，講者提出數個改善建議，如引導使用者選擇有利於隱私的選項、預設開啟隱私區域並依街道密度提升端點隱私區域所遮蔽之範圍等方式。講者及研發團隊亦將此攻擊發現分享給相關社群服務提供者，將共同研究並更好的隱私保護方式，以期望使用者們在享受健身社交網路帶來的好處時，也能保護其個人隱私。

十、Phoenix Domain Attack: Vulnerable Links in Domain Name Delegation and Revocation（鳳凰網域攻擊：網域委派和撤銷中的弱點連結，講者：Xiang Li）

網域名稱即是網際網路活動的入口，也是各種應用服務的網路門牌。然而，網域名稱經常被用於犯罪活動，例如構建僵屍網絡、釣魚攻擊和惡意軟件分發。為了彰顯這種網域名稱濫用狀況，ICANN（網際網路名稱與數字位址分配機構，Internet Corporation for Assigned Names and Numbers）在 2023 年 3 月提出了網域名稱濫用活動報告（DAAR，Domain Abuse Activity Reporting），於該報告中說明有近 63 萬個網域名稱存在資安威脅。

為了對抗惡意網域名稱，吊銷網域名稱成為一種重要的機制。通過由註冊機構或註冊商的操作下，可以刪除或更改網域名稱註冊資訊，使網域名稱不再受原註冊者或攻擊者控制。

即使如此，吊銷網域名稱仍然存在資安漏洞，在 2012 年的 NDSS（網路和分散式系統安全研討會，Network and Distributed System Security Symposium）會議上，清華大學網絡與信息息安全實驗室提出了幽靈網域（Ghost Domain）攻擊，該攻擊使應被吊銷的網域名稱仍然可以在 DNS 上被解析，使攻擊者可以繞過吊銷網域名稱或網域名稱到期的操作，進而繼續影響資訊安全。

幽靈域名攻擊主要利用易受攻擊的 DNS 漏洞，於 DNS 中網域名稱尚在保留期限內的舊 NS 紀錄，插入新的 NS 紀錄，即可再次延長原先應過期而準備刪除

的網域名稱(圖 46)。

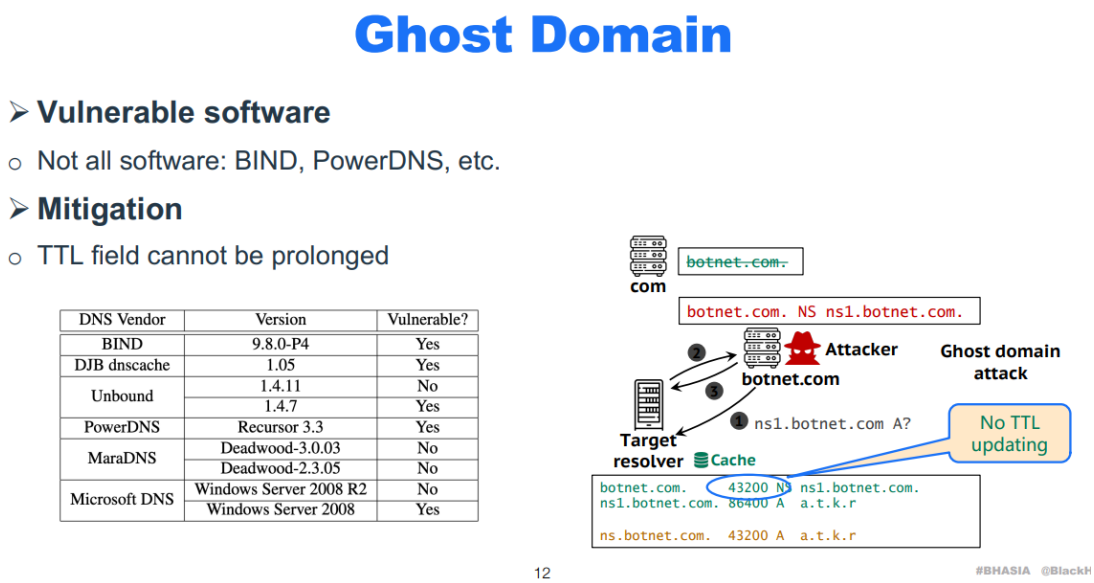
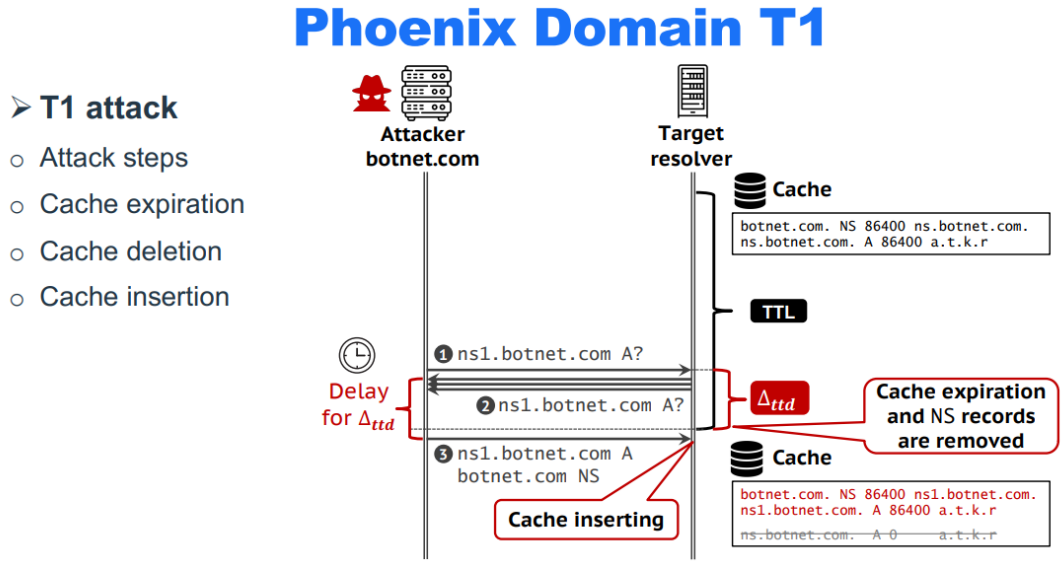


圖 46. 幽靈網域運作方式及受影響的 DNS 版本（資料來源：講者簡報）

近期同樣由清華大學網絡與信息安全實驗室提出鳳凰網域（Phoenix Domain）攻擊，其有兩種模式，第一種方法是攻擊者在 DNS 回應完 A 紀錄後，就故意在 DNS 等待 TTL 回應逾時並刪除了 NS 紀錄，才再利用漏洞插入新的 NS 紀錄進入 DNS 伺服器的快取中（圖 47）；第二種方法是利用 DNS 伺服器的漏洞，可插入上百層子網域名稱供使用（圖 48）。



上一頁圖 47．鳳凰網域攻擊模式 1，利用等待逾時再插入新 NS 紀錄（資料來源：講者簡報）

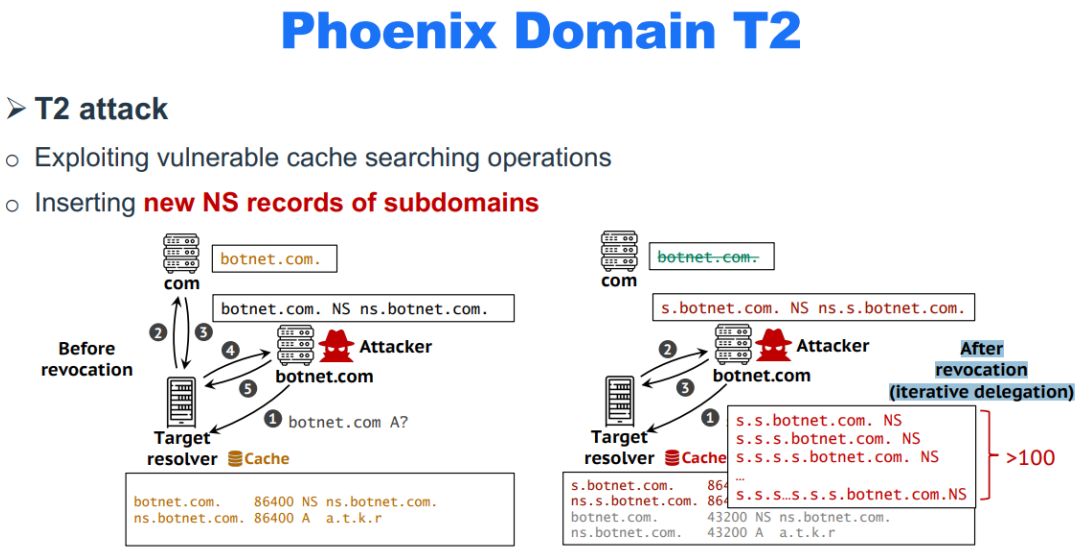


圖 48．鳳凰網域攻擊模式 2，利用漏洞插入多層子網域（資料來源：講者簡報）

多個軟體和公共 DNS 包含 Google Public DNS 和 Cloudflare DNS 皆易受到這些攻擊，現今所有受影響的供應商都已確認漏洞的存在，已在研究問題並發佈緩解修補版本，為了緩解這些漏洞，講者提出了多種建議，例如在 NS 紀錄過期時向上游查詢、更信任來自父域的 NS、使用較小的 TTL 值等方式。

總結來說，吊銷網域名稱的漏洞給網際網路安全帶來了風險。DNS 的規範並未明確定義每個操作，因此留下了攻擊的機會，且不同軟體的 DNS 實作模式有所不同，這可能隱藏了其它潛在的風險，原始的 DNS 機制對於抵擋多種攻擊類型是不足的，講者建議提出新的修補程式或重新設計結構來改進 DNS 的安全性。

十一、Cloudy With a Chance of Exploits: Compromising Critical Infrastructure Through IIoT Cloud Solutions（雲端服務中的風險：透過工業物聯網雲端解決方案所危及的關鍵基礎設施，講者：Roni Gavrilov）

現今工業已從 1.0 機械化進展到 4.0 也就是所謂的「第四次工業革命」，此次革命旨在於「智慧製造」，其包含了 IOT（Internet of Things）、大數據和 AI，講者以此著重探討使用工業物聯網（IIoT，Industrial Internet of Things）雲解決方案時可能遭遇的風險，隨著物聯網技術的普及，工業企業的營運和經濟效益得到了巨大的提升，但也帶來了新的風險和挑戰。其中一個重大風險是存在於雲端問題，在工業遠端登入情境中，使許多工業公司過度暴露於單一 IIoT 供應商的安全風險中。

現今 IIoT 供應商提供雲端的管理解決方案，多用於遠程管理和操作設備，講者在研究中重點關注了三個主要 IIoT 雲端供應商（Sierra Wireless、Teltonika Networks 和 InHand Networks）的雲端管理平台，在調查它們可能受到惡意行為利用的方式時，發現了這些類型的平台可以成為訪問多個工業和關鍵環境的後門。

講者展示通過雲端管理的 IIoT 設備受到攻擊的模式，發現的漏洞將影響工業環境中的數千個設備，繞過 NAT 並通過網路遠端程式碼執行（RCE，remote code execution），直接到達內部網路（圖 49）。以此引起人們對工業物聯網雲解決方案的安全性問題的關注。強調了過度依賴於雲端管理的風險，以及由於這些解決方案可能存在的漏洞和攻擊向量所帶來的潛在威脅。

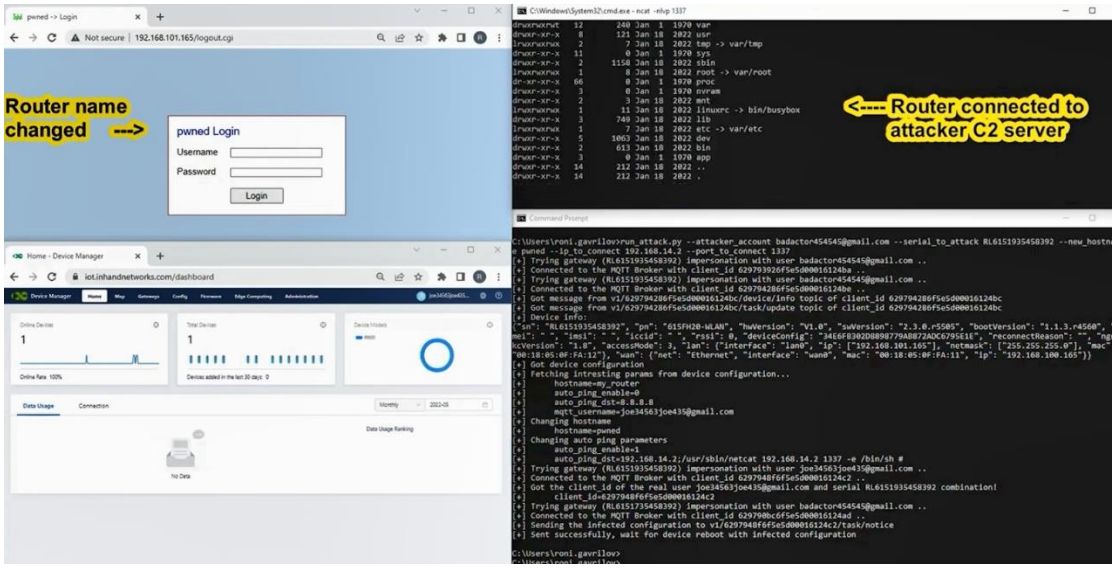


圖 49．展示遠端程式碼執行（資料來源：講者簡報）

講者期望人們理解 IIoT 雲解決方案的風險和潛在威脅，希望促使相關業者能加強對這些解決方案的安全性管理和保護，只有通過合理的安全措施和策略，工業企業才能充分利用 IIoT 技術的好處，同時保護其關鍵基礎設施免受潛在的攻擊和破壞。

肆、心得與建議事項

本次黑帽駭客活動集結了全球頂尖的資安專家和研究人員，分享了最新的安全漏洞和攻擊技術，黑帽活動提供了一個寶貴的學習平台，無論是在技術展示、工作坊還是演講中，都可讓學員學習到各種攻擊手法、防禦機制與數位鑑識技術。在工作坊中，講師 Monnappa KA 在惡意程式解析的領域中具有數年經驗之專家，在課程「 A Complete Practical Approach to Malware Analysis and Memory Forensics - 2023 Edition」中從靜態分析到動態分析；從程式碼到惡意程式解析，在講師以由淺入深的方式，引領學員深入了解系統的運作方式，同時使用不同工具進行實機演練，其中許多實用的技巧和工具操作，在執行數位證據的保全工作，並取得可疑程式後，即可運用課程中的工具進行檢測和鑑識，以判斷該程式是否為惡意程式。

本次黑帽駭客活動研討會中所分享的各式資安議題裡，每位講者都有不同的主題和研究，以下則從參與的演講中提出幾點值得關注的資安議題及建議：

(1)網路攻擊自動化：

在「When Knowledge Graph Meets TTPs: Highly Automated and Adaptive Executable TTP Intelligence for Security Evaluation（當知識圖譜遇上 TTPs：高度自動化和適應性執行 TTP 智能安全評估）」的演講中，講者除了展示推理引擎的攻擊模式已可透過知識圖譜來強化，進而使自動化安全評估用的攻擊系統更具發現系統弱點的能力，但反方面來說，若系統開始導入 AI，並由駭客來做攻擊使用時，將可能引發多種問題，故未來在研發此系統時，應為此系統增加使用認證或是偵測特定 port 有開通才攻擊等方式，來降低被盜用之可能性。

(2)IOT 及 IIOT 之防禦：

在「Cloudy With a Chance of Exploits: Compromising Critical Infrastructure Through IIoT Cloud Solutions（雲端服務中的風險：透過工業物聯網雲端解決方案所危及的關鍵基礎設施）」中提及現今工業裡，使用 IIOT，其搭配雲端物聯網是現今工業提升營運及經濟效益的方式之一，其方便性中帶來的資安隱憂是目前 IIOT 雲端供應商急需面對並解決的，而在「Sweet Dreams: Abusing Sleep Mode to Break Wi-Fi Encryption and Disrupt WPA2/3 Networks（甜美夢境：濫用睡眠模式破解 Wi-Fi 加密並干擾 WPA2/3 網路）」演講中所提及的 Wi-Fi 加密破解，則是各種使用 Wi-Fi 的 IOT 設備或各種無線 AP 都要面對的問題，故提升系統安全性並強化安全措施是勢在必行，應加強各種 IOT 設備的 CVE 漏洞的偵測與修補以降低系統遭駭之可能性。

(3)DNS 防護：

在「Phoenix Domain Attack: Vulnerable Links in Domain Name Delegation and Revocation（鳳凰網域攻擊：網域委派和撤銷中的弱點連結）」中，講者介紹了 Ghost Domain 及 Phoenix Domain 的兩種攻擊，其方式都是能在現今 DNS 服務造成一定的影響，除了系統廠商應盡速強化防護的機制及修補漏洞外，也應考慮 DNS 防護機制或是推廣能降低被影響的保護措施。

(4)資料及個資的保護：

在現今的社會裡，資料透過網路變得容易取得，而個人資料或機敏資料則是極易流失，在「A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks（每天慢跑無法阻止駭客：對健身追踪社交網路中終端隱私區域的推論攻擊）」演講中可發現雖然社交網路系統業者有注重個

人隱私，並以端點隱私區域（EPZ，Endpoint Privacy Zones）技術來保護個人住址的個資，但卻仍逃不過推論演算的攻擊而被發現使用者的實際住所，故講者建議應依居住密度而加強隱私防護範圍或是再增強其它防護方式。而在「Insider Threats Packing Their Bags With Corporate Data（將企業數據打包的內部威脅）」中則是以統計的方式來找出企業資料因離職人員而外洩的可能發生時間，推估出離職人們中約有 2%的人裡會在離職前 50 天內做出資料移轉外洩的可能性，講者以此數據建議應加入異常行為檢測、資料標籤和資料損失防護（DLP）技術來識別和保護敏感檔案。放眼國內，我們應也思考是否在機關內，考慮在機敏檔案或是設備增加防護及偵測的機制，以確保資料安全。

本次資安活動除了介紹各種先進的攻擊技術和利用漏洞的手法，也不時的提醒我們，無論是個人用戶還是企業組織，都必須時刻保持警惕並採取適當的防護措施來保護我們的系統和資料，資安攻擊不僅僅是企業或是組織的問題，而是全民都要面臨的挑戰！

因應資通安全攻擊手法日益進化，資安事件鑑識工作亦日趨重要，未來除可逐步提升我國資安人員數位鑑識能力，以駭客思維，學習以攻擊者的角度挖掘資安的問題，並透過國際資安交流活動，瞭解最新資安趨勢，作為我國擬定相關政策之參考，持續強化我國資安防護能量。